

# (12) UK Patent Application (19) GB (11) 2 338 815 (13) A

(43) Date of A Publication 29.12.1999

(21) Application No 9914847.0

(22) Date of Filing 24.06.1999

(30) Priority Data

(31) 09104702 (32) 25.06.1998 (33) US

(71) Applicant(s)

**Mr Payroll Corporation**  
(Incorporated in USA - Texas)  
534 Fourth Street, San Francisco,  
California 94107-1621, United States of America

(72) Inventor(s)

**Michael C Stinson**  
**John W Templer Jr**  
**Dyron Clower**

(74) Agent and/or Address for Service

**D Young & Co**  
21 New Fetter Lane, LONDON, EC4A 1DA,  
United Kingdom

(51) INT CL<sup>6</sup>  
G07F 19/00

(52) UK CL (Edition Q )

G4V VAK  
G4H HTG  
G4X X5

(56) Documents Cited

EP 0878780 A2 WO 98/35298 A1 WO 98/15924 A2  
US 5386104 A

(58) Field of Search

UK CL (Edition Q ) G4H HTG , G4V VAK , G4X X5  
INT CL<sup>6</sup> G07C 9/00 , G07F 7/10 19/00  
Online: WPI, EPODOC, JAPIO

(54) Abstract Title

**ATM with biometric verification**

(57) An ATM 160 includes an input device, such as a numeric keypad 110, card reader 145 or touch screen 105, a biometric input device such as a digital camera 125, a storage device which includes a customer database, and an electronic processor which compares biometric input data with stored data, contacts a verification network to request authorization for a cash advance, and approves the cash advance subject to authorization. The ATM may include a cheque reader 130, two cameras 125, lights 155, a microphone 120, a speaker 115 and a voice synthesizer. The ATM may be able to cash cheques and approve loans, and may be able to contact a human operator at a service centre for assistance. The biometric information may include data taken from a users face, palm, fingers, iris, retina, DNA, or voice.

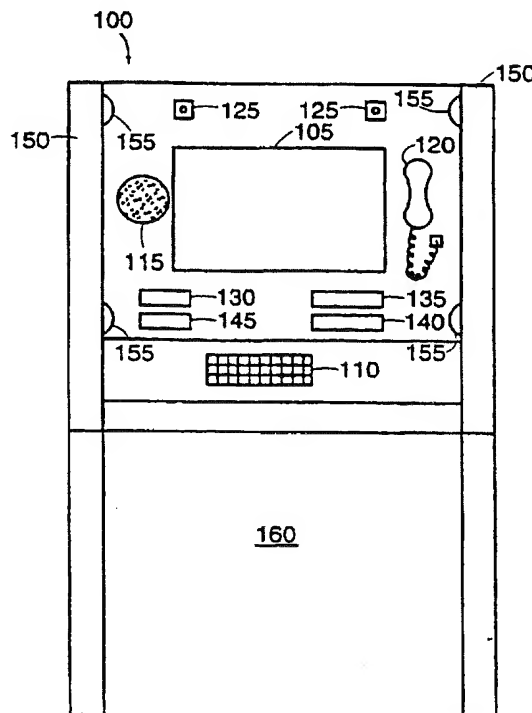


FIG. 1

GB 2 338 815 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

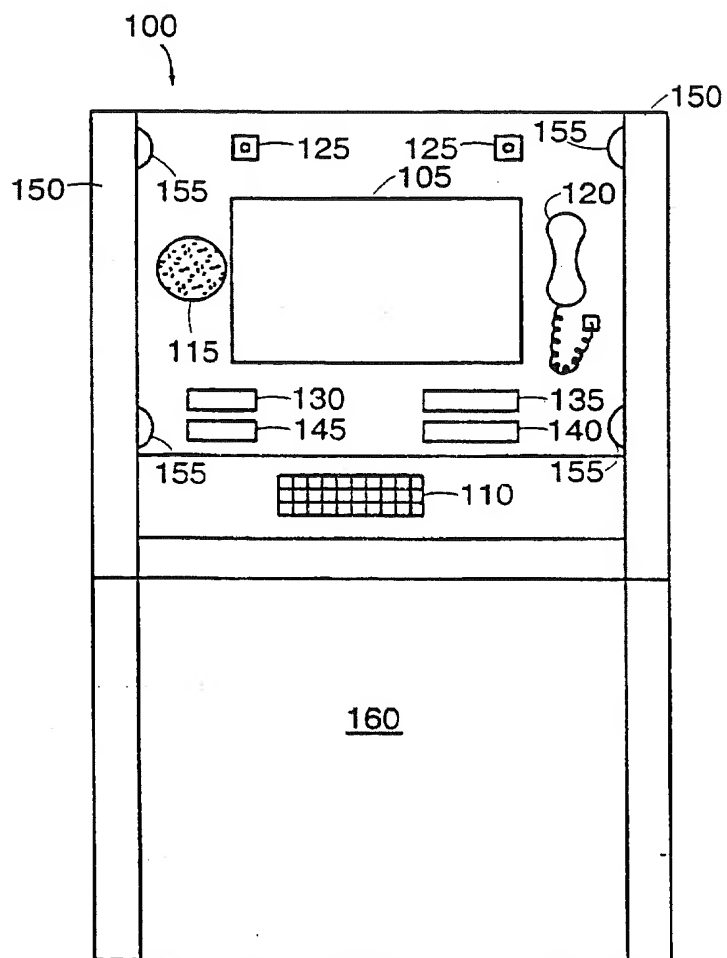


FIG. 1

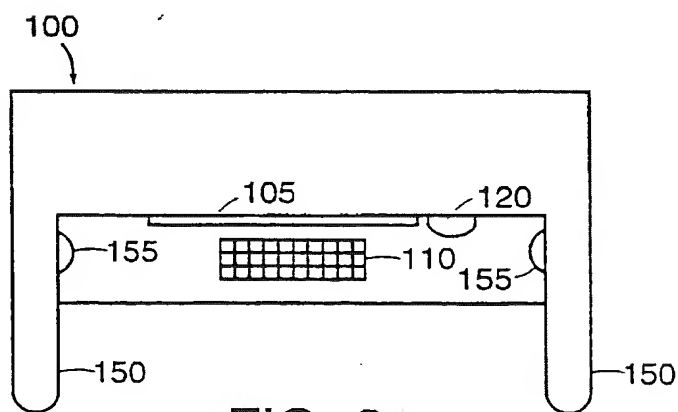
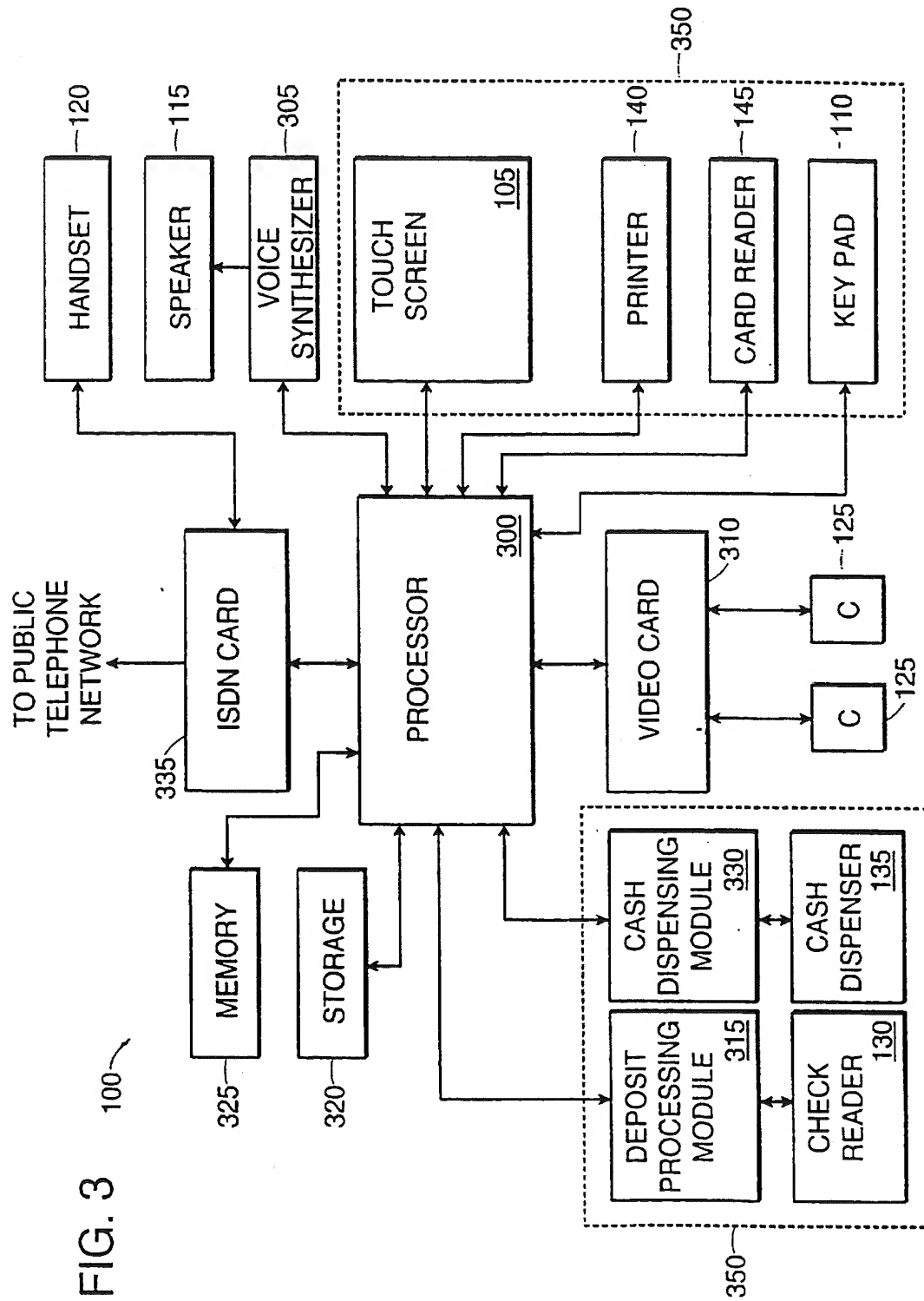


FIG. 2



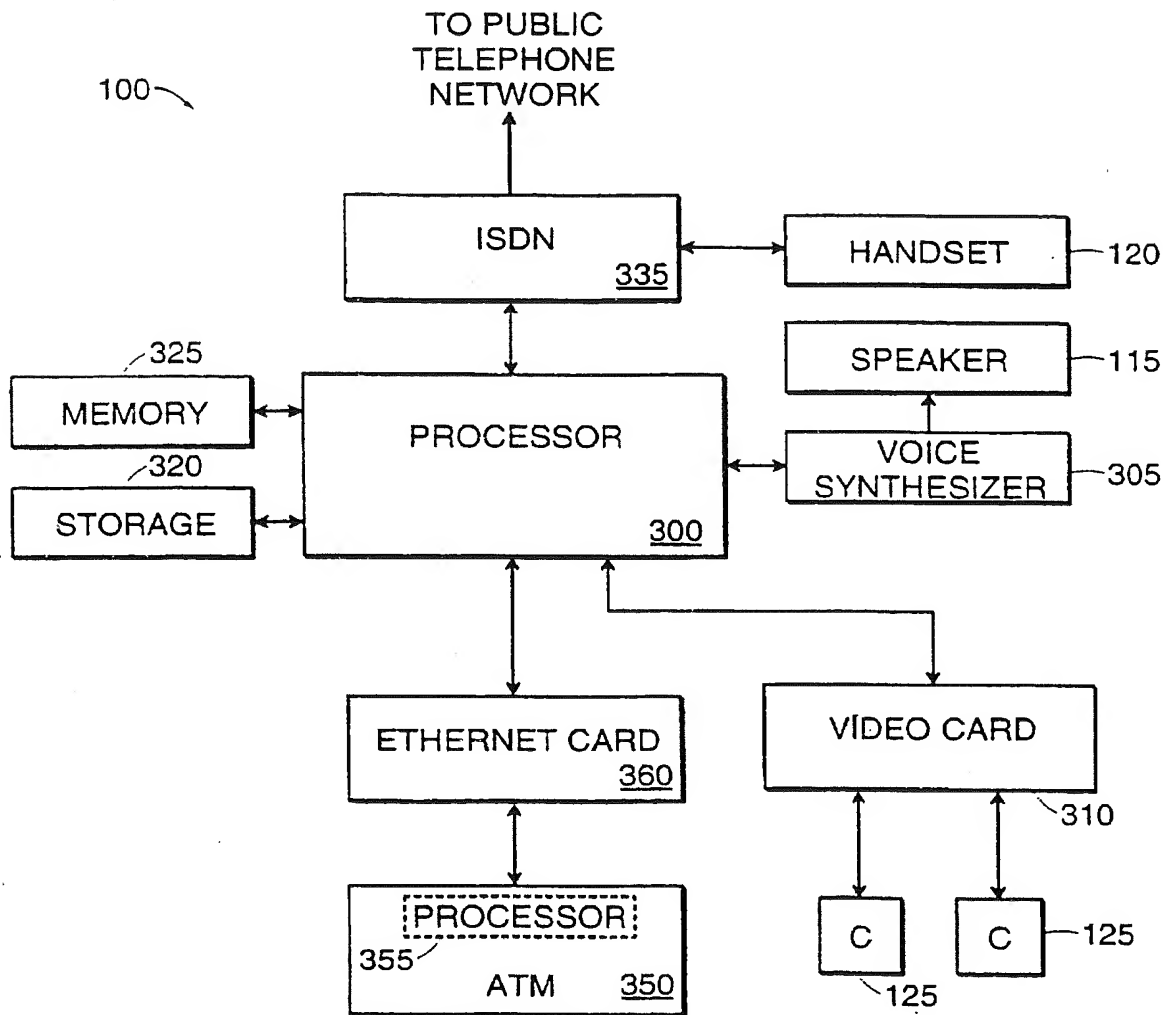


FIG. 3A



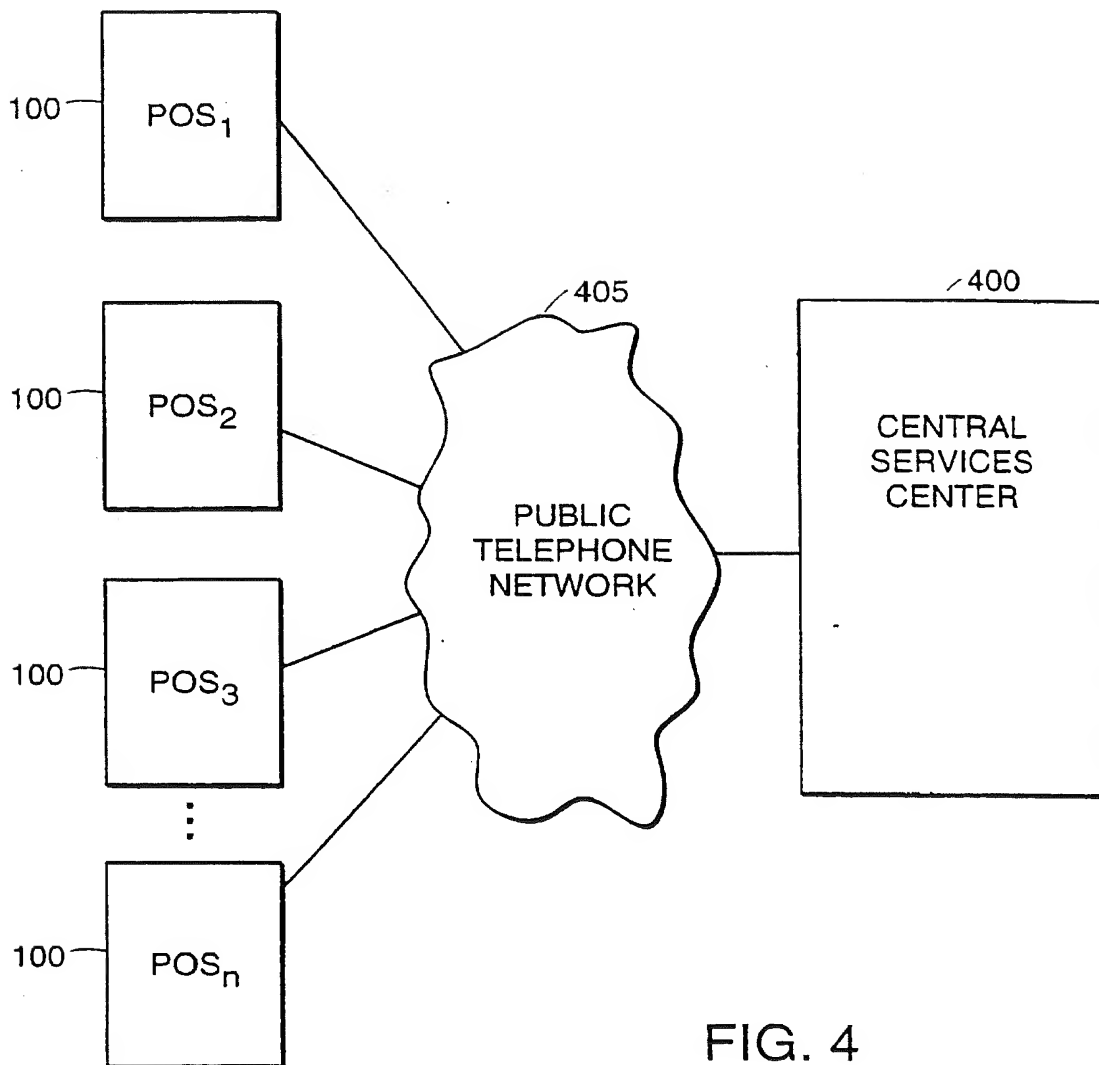


FIG. 4

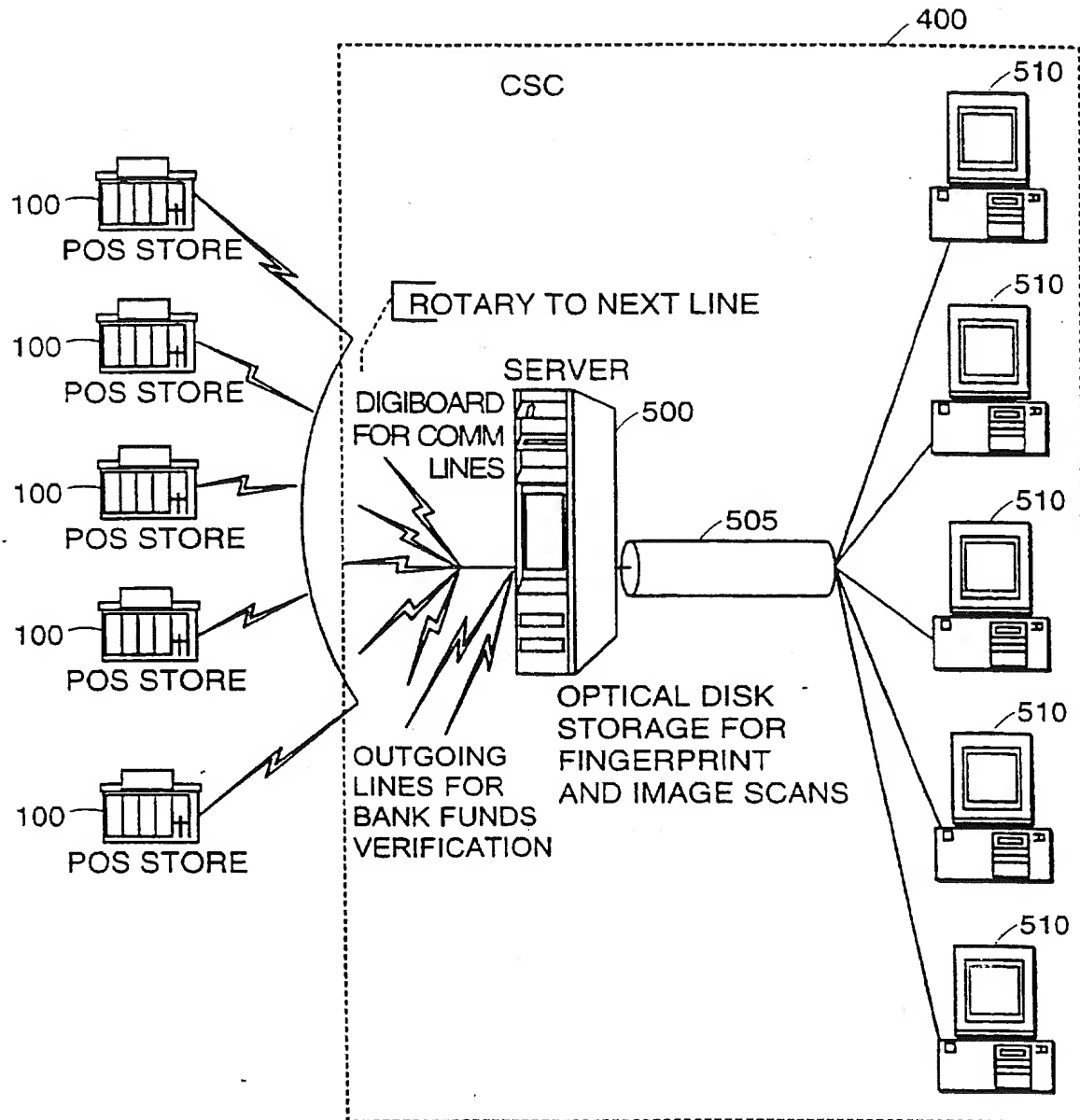
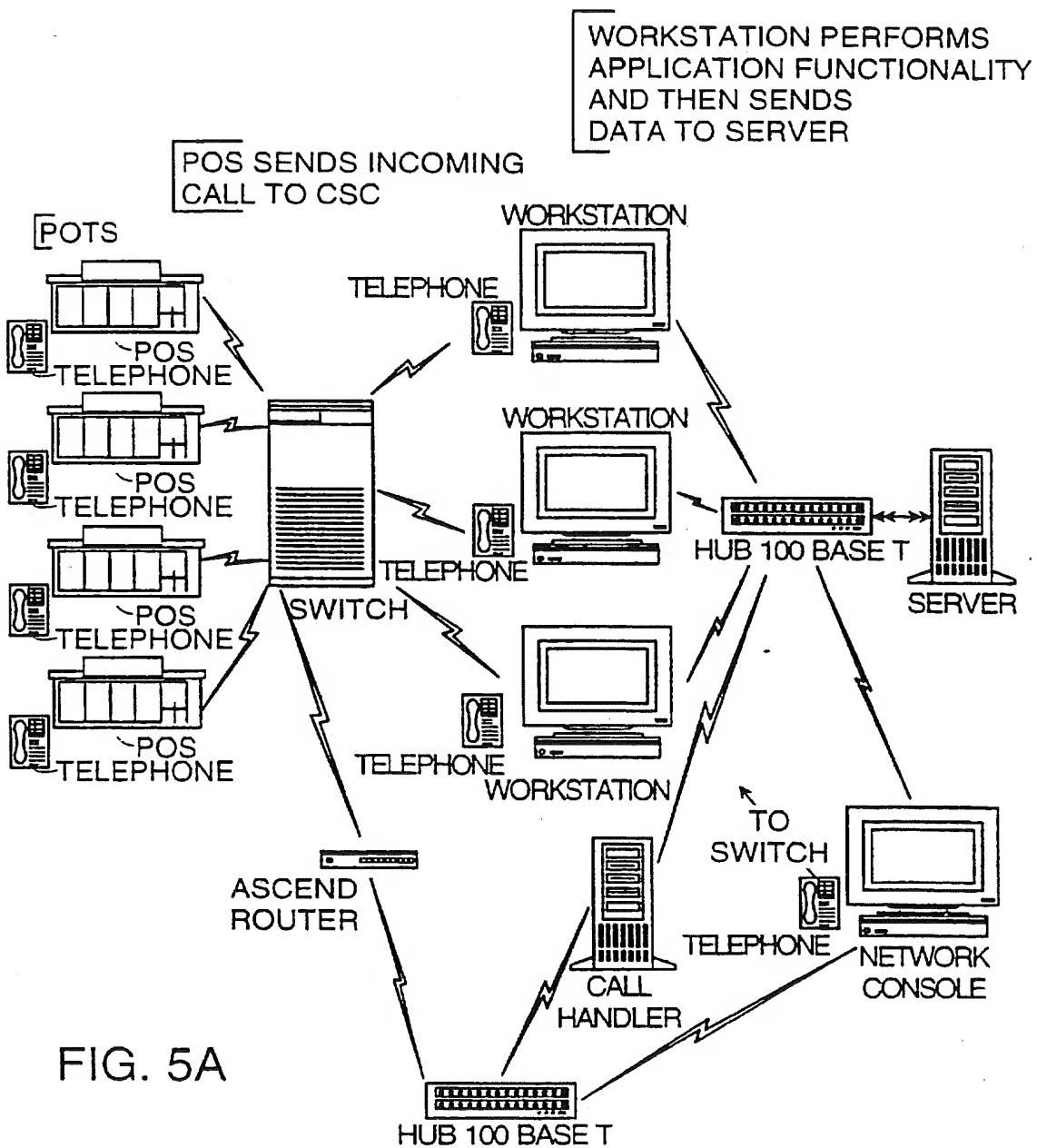


FIG. 5



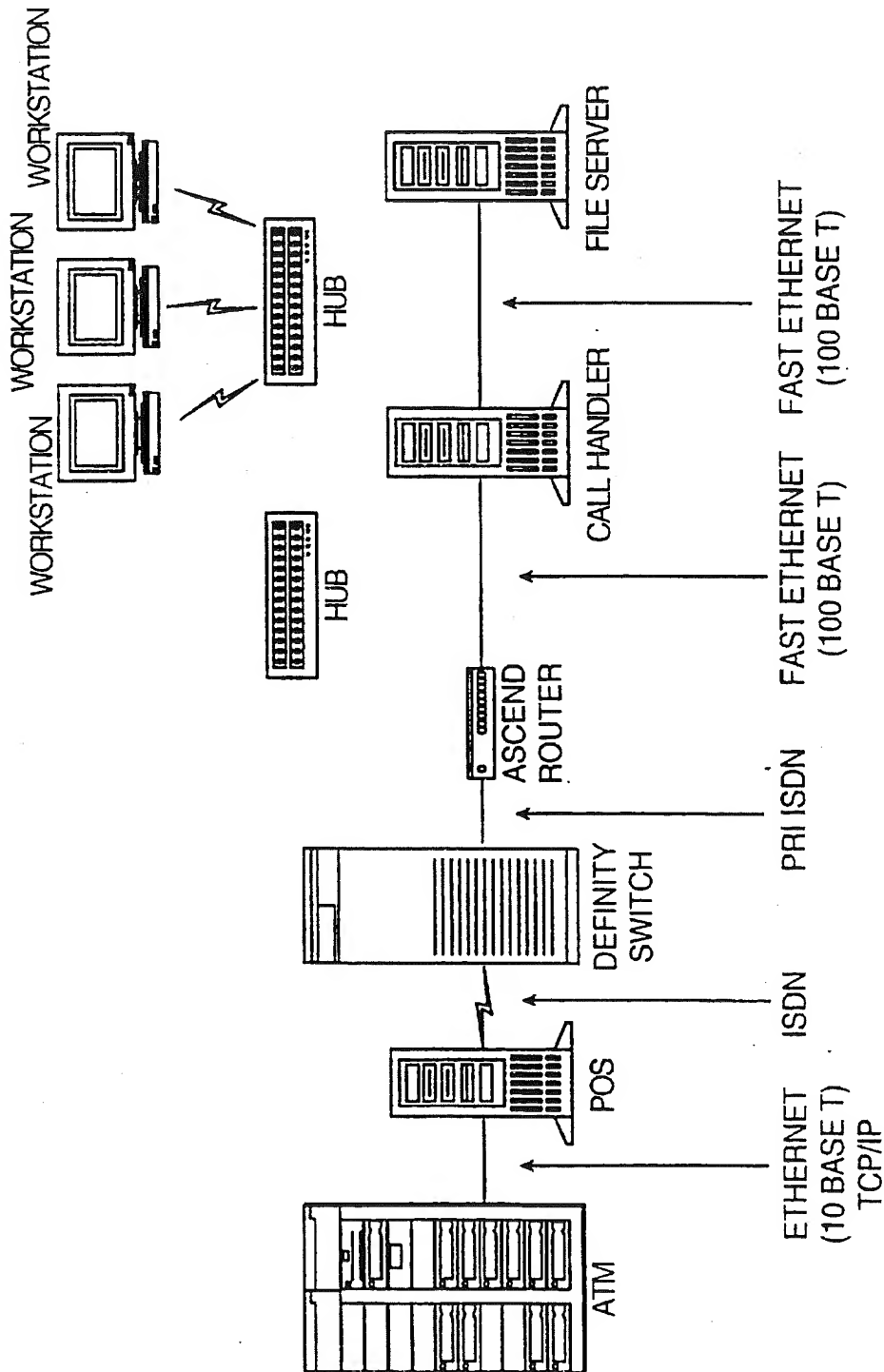


FIG. 5B

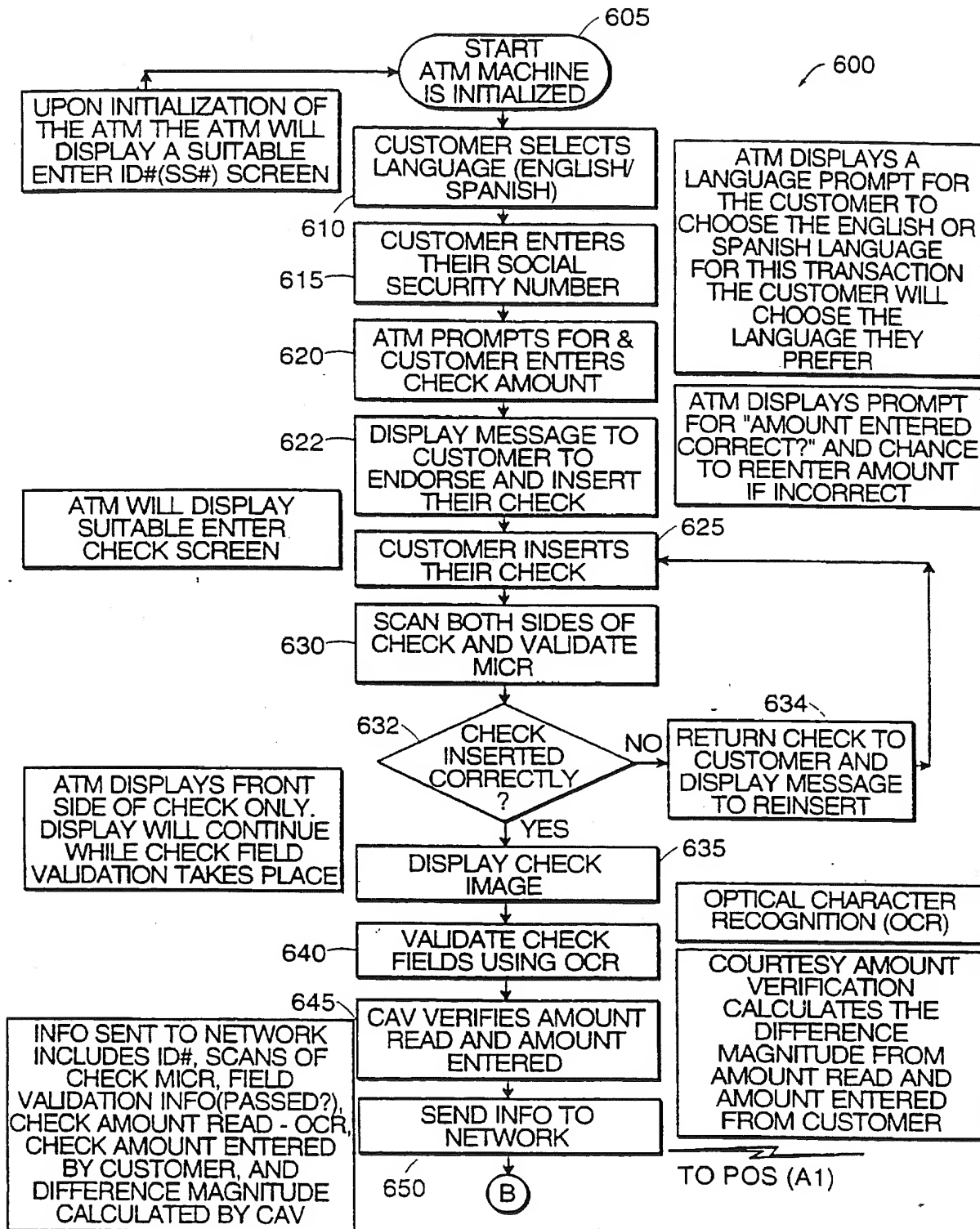


FIG. 6A

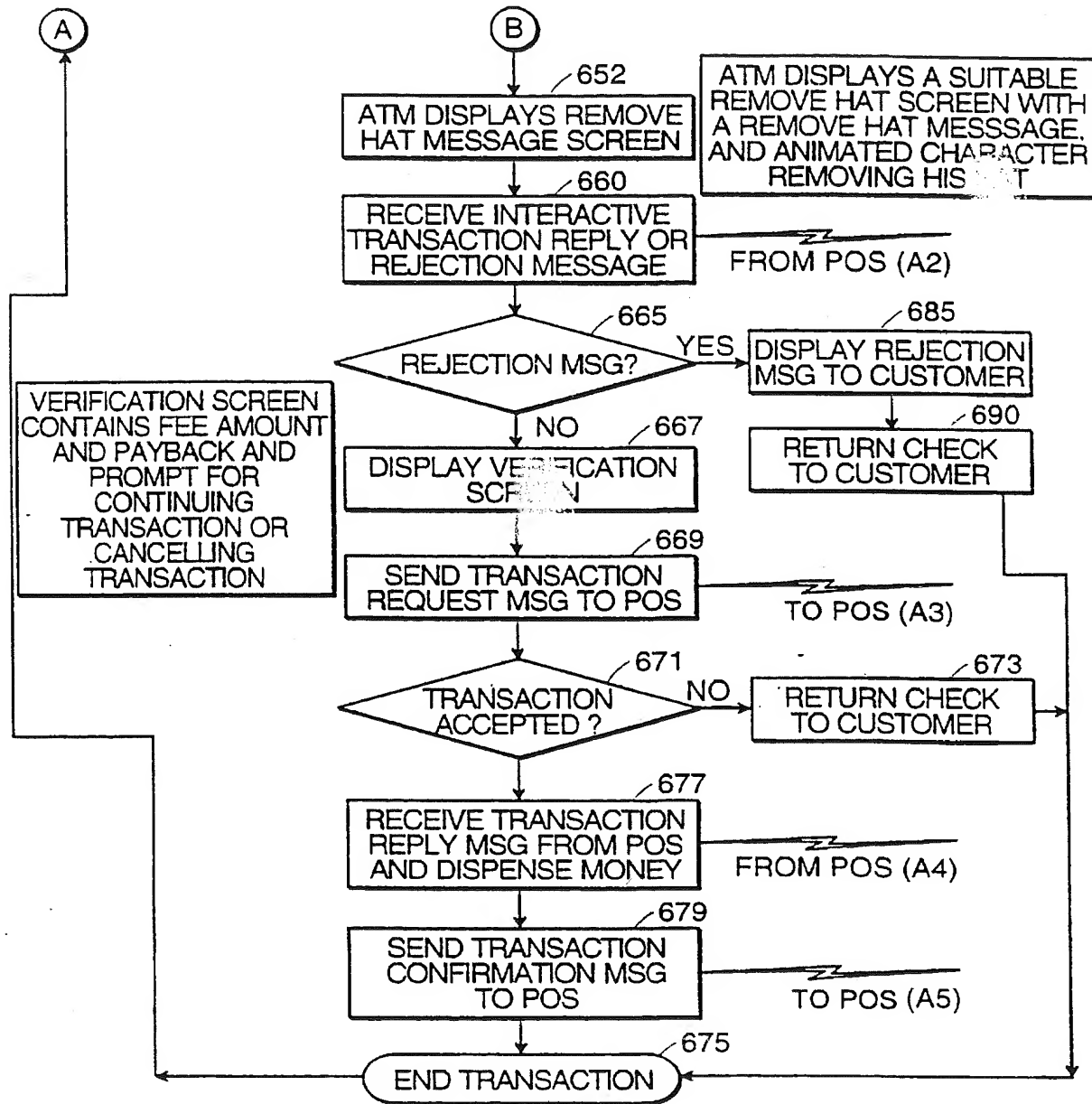
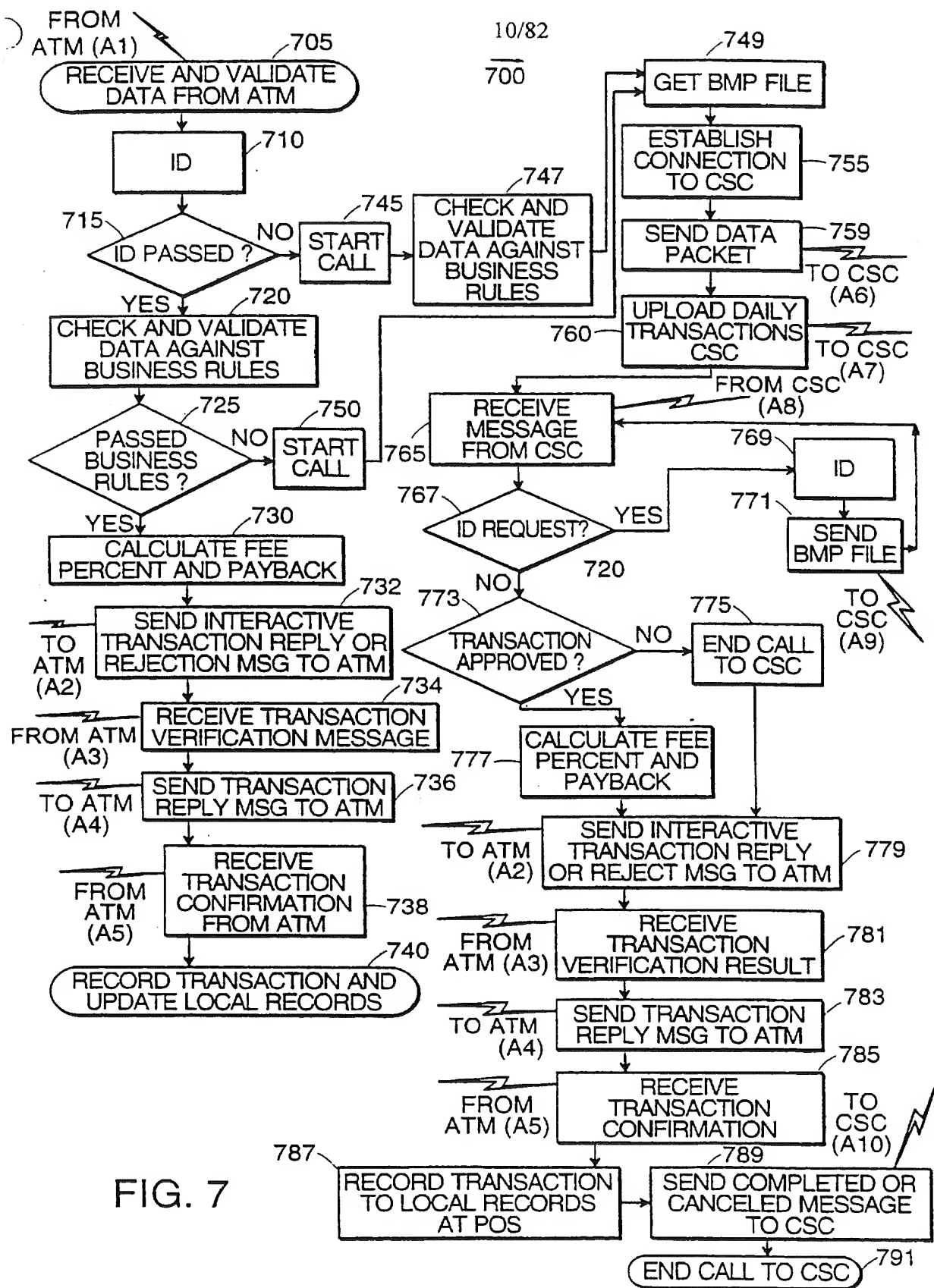


FIG. 6B



11/82

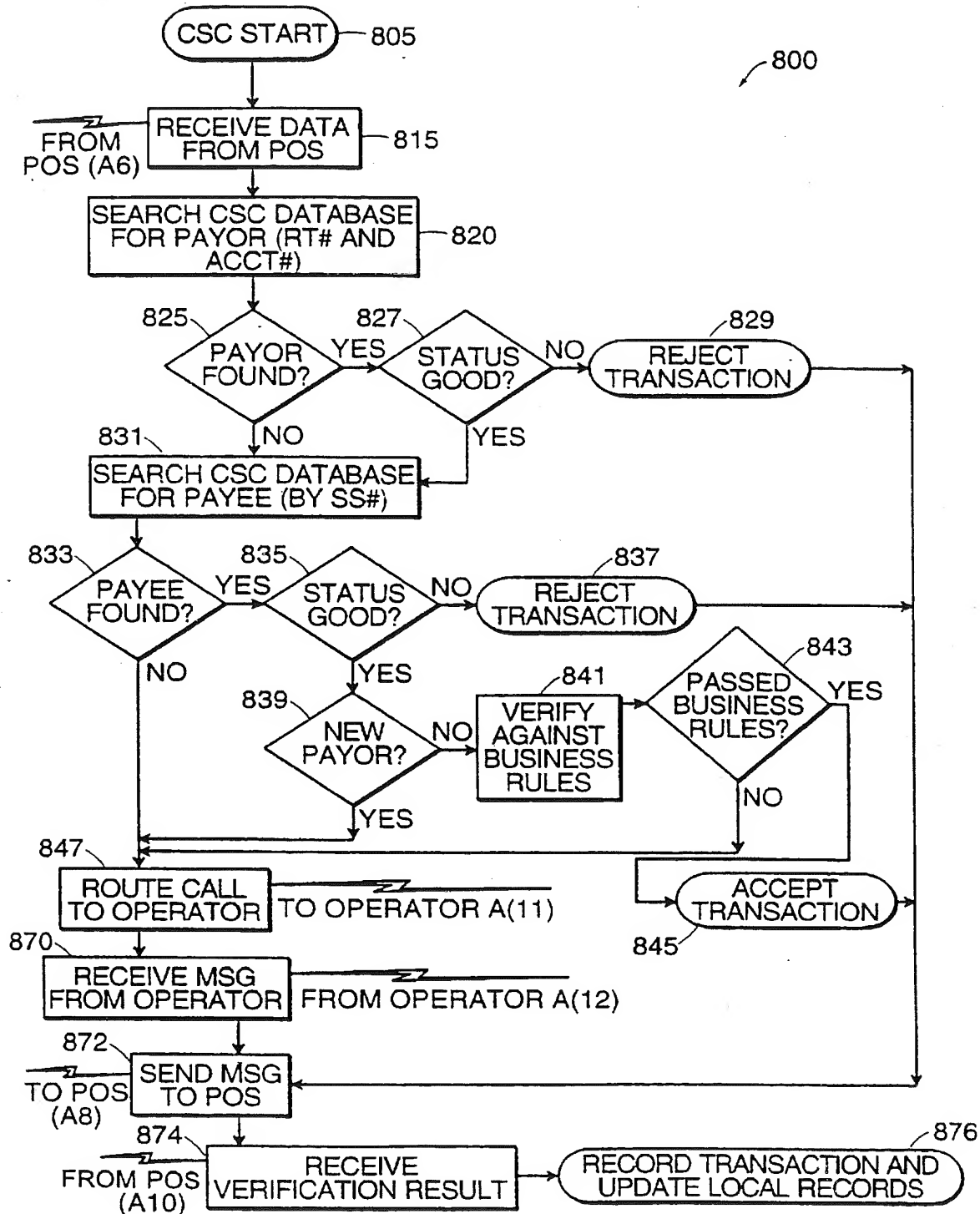


FIG. 8A



12/82

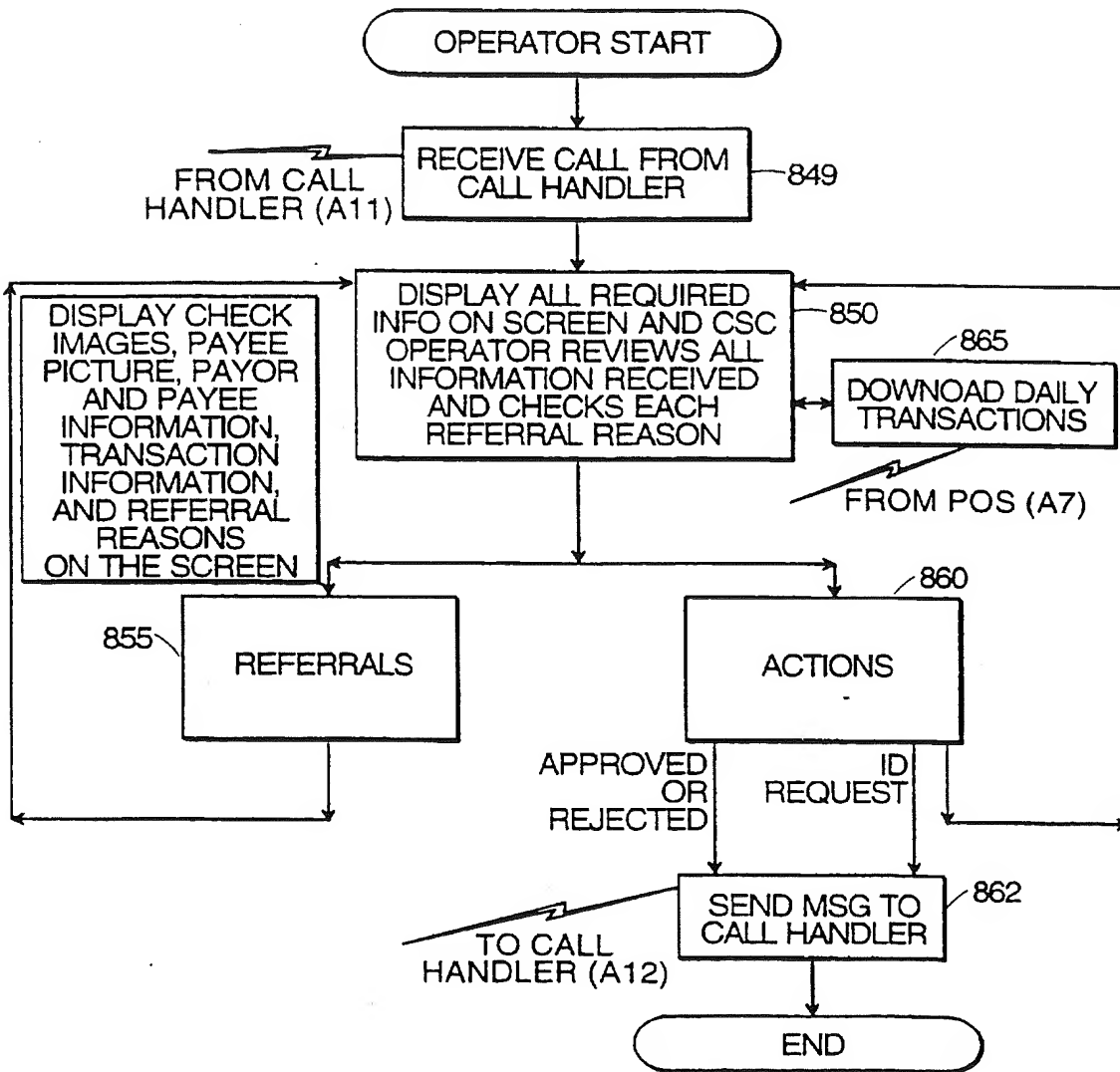


FIG. 8B

CRITERIA	VALUE
AMOUNT OF CHECK	IF ONE OF THE FIRST 4 CHECKS CASHED FOR THE PAYEE CAN'T BE MORE THAN 15% OF ANY OF THE PREVIOUS CHECKS
AMOUNT OF CHECK	IF AFTER THE 4 CHECK FOR THE PAYEE CAN'T BE MORE THAN 25% OF ANY OF THE PREVIOUS CHECKS
AMOUNT OF CHECK	IF CHECK EXCEEDS SET LIMITS
CHECK ENDORSEMENT	IF CHECK ENDORSEMENT IS NOT FOUND
CAV COMPARISON	IF AMOUNT READ BY OCR MODULE DIFFERS FROM AMOUNT ENTERED BY CUSTOMER, SEND TO CSC
PAYOR	IF NEW PAYOR
PAYOR	STATUS OF VERIFY
PAYOR LAST TRANSACTION DATE	IF OVER 33 DAYS SINCE LAST TRANSACTION
PAYOR	IF FILE IS TAGGED TO ALWAYS GO TO CENTRAL
PAYEE	IF NEW PAYEE
PAYEE	STATUS OF VERIFY
PAYEE'S LAST TRANSACTION DATE	IF ONE OF THE FIRST 4 CHECKS FOR THE PAYEE CASHED CAN'T BE LESS THAN 6 OR GREATER THAN 18 DAYS
PAYEE	FIRST 2 TRANSACTIONS ON PAYOR PROBATIONARY PERIOD
PAYEE'S LAST TRANSACTION DATE	IF AFTER THE 4 CHECKS FOR THE PAYEE CAN'T BE LESS THAN 6 OR GREATER THAN 63 DAYS
PAYEE'S BIOMETRIC IMAGE	DOES NOT MATCH
MICR	MICR DOES NOT READ PROPERLY
ATM	CASH MACHINE HAS INSUFFICIENT FUNDS FOR CURRENT TRANSACTION
CHECK NUMBER	DUPLICATE CHECK NUMBER
POS LAST COMMUNICATION DATE	POS LAST COMMUNICATION DATE WITH CSC IS GREATER THAN 7 DAYS

FIG. 9

CENTRAL SERVICES CENTER			
<b>PAYOR INFORMATION</b> NAME START DATE LAST TRANS DATE # OF RETURNED CHECKS		<b>PAYOR/PAYEE INFORMATION</b> AVG. CHECK AMT. AVG. CHECKS CASHED PER WEEK # CHECKS CASHED	
<b>PAYEE INFORMATION</b> FROM POS ON FILE LAST NAME FIRST NAME START DATE LAST TRANS DATE # OF RETURNED CHECKS F5 TO VIEW ADDITIONAL PAYEES FOR THIS CHECK			
<b>TRANSACTION INFORMATION</b> STORE: ID SS# DOB ACCT# CHECK# AMOUNT FEE% FEE PAYBACK			
<div style="border: 1px solid black; padding: 10px; text-align: center;"> CHOOSE PAYOR MAINTENANCE BUTTON,  EDIT OR ENROLL PAYOR, OR VIEW EXISTING  PAYOR INFORMATION </div>			
<div style="display: flex; justify-content: space-between;"> <div> <b>BACK:</b>  <div style="border: 1px dashed black; width: 100px; height: 100px;"></div> </div> <div> <b>FRONT:</b>  <div style="border: 1px dashed black; width: 100px; height: 100px;"></div> </div> </div>			
<b>OPTIONAL ACTIONS:</b> PAYOR MAINTENANCE PAYEE MAINTENANCE SS# SEARCH PAYEE HISTORY PAYOR HISTORY TRANSACTION MAINT. RETAKE PICTURE CALL CUSTOMER ACCEPT REJECT			
<b>MANDATORY ACTIONS:</b> PAYOR MAINTENANCE PAYEE MAINTENANCE SS# SEARCH VERIFY FUNDS CALL MAKER SUPERVISOR APPROVAL CHECK ID VERIFY CHECK CHECK ENDORSEMENT CALL CUSTOMER			
REF1 REF2 REF3 REF4 REF5 REF6 REF7 REF8 REF9 REF10 REF11 REF12 REF13 REF14 REF15 REF16 REF17 REF18 REF19			

FIG. 10

☐ PAYEE SEARCH

PLEASE TYPE IN THE PAYEE NAME: FIND:

FIG. 11A

☐ PAYOR SEARCH

PLEASE TYPE IN THE PAYOR NAME: FIND:

FIG. 11B

PAYEE MAINTENANCE			
SS#:	<input type="text"/>	STATUS:	<input type="text"/> <input type="button" value="v"/>
		<input type="button" value="ADD ANOTHER PAYEE"/> <input type="button" value="CLOSE"/>	
LASTNAME:	<input type="text"/>		
FIRSTNAME	<input type="text"/>		
MIDDLENAME:	<input type="text"/>		
PHONE:	<input type="text"/>		
ADDR1:	<input type="text"/>		
ADDR2:	<input type="text"/>		
CITY:	<input type="text"/>	ST:	<input type="text"/>
DOB:	<input type="text"/>	ZIP:	<input type="text"/>
SEX:	<input type="text"/>		
NOTES:	<input type="text"/>		
STARTDATE:	<input type="text"/>		
LAST UPDATE DATE:	<input type="text"/>		
LAST UPDATE TIME:	<input type="text"/>		

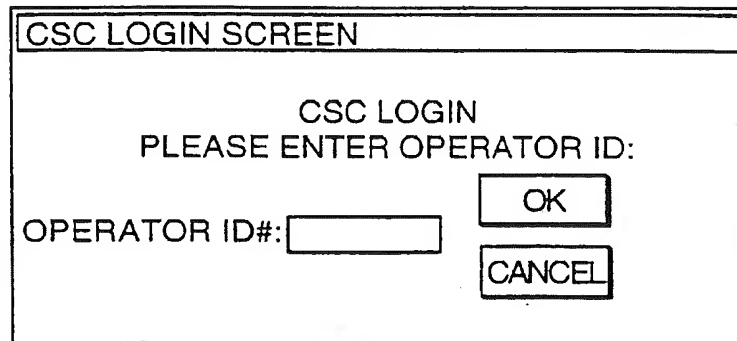
FIG. 11C

PAYOR MAINTENANCE					
RT#:	<input type="text"/>	ACCT#:	<input type="text"/>	<input type="button" value="CLOSE"/>	
FEDERAL ID#:	<input type="text"/>	STATUS:	<input type="text"/>	<input type="button" value="v"/>	
NAME:	<input type="text"/>				
ADDR1:	<input type="text"/>				
ADDR2:	<input type="text"/>				
CITY:	<input type="text"/>	ST:	<input type="text"/>	ZIP:	<input type="text"/>
PHONE:	<input type="text"/>				
CHECKTYPE:	<input type="text"/>				
STARTDATE:	<input type="text"/>				
NOTES:	<input type="text"/>				
LAST UPDATE DATE:		<input type="text"/>			
LAST UPDATE TIME:		<input type="text"/>			

FIG. 11D

SUPERVISOR APPROVAL	
PLEASE ENTER SUPERVISOR CODE:	
<input type="text"/>	
<input type="button" value="OK"/>	<input type="button" value="CANCEL"/>

FIG. 11E

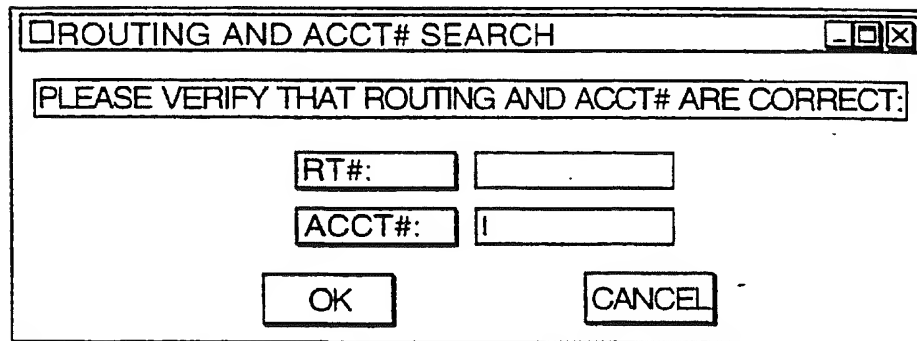


CSC LOGIN SCREEN

CSC LOGIN  
PLEASE ENTER OPERATOR ID:

OPERATOR ID#:

FIG. 11F



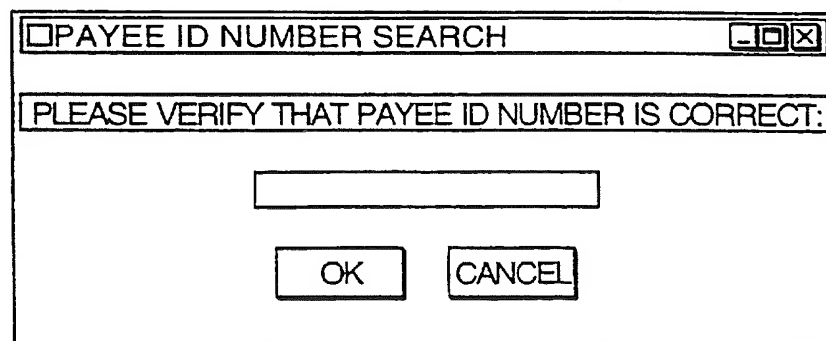
☐ ROUTING AND ACCT# SEARCH

PLEASE VERIFY THAT ROUTING AND ACCT# ARE CORRECT:

RT#:

ACCT#:

FIG. 11G

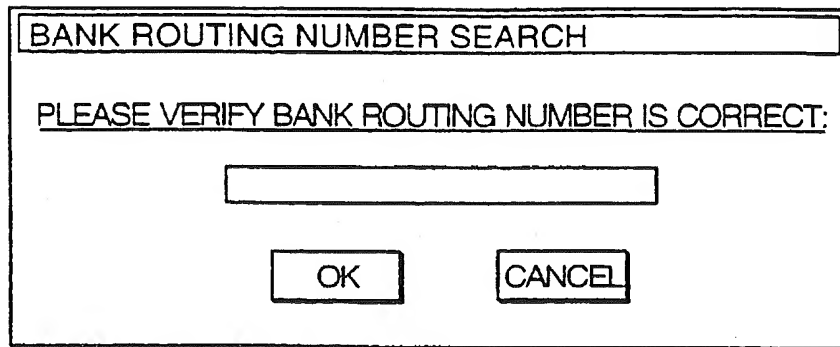


☐ PAYEE ID NUMBER SEARCH

PLEASE VERIFY THAT PAYEE ID NUMBER IS CORRECT:

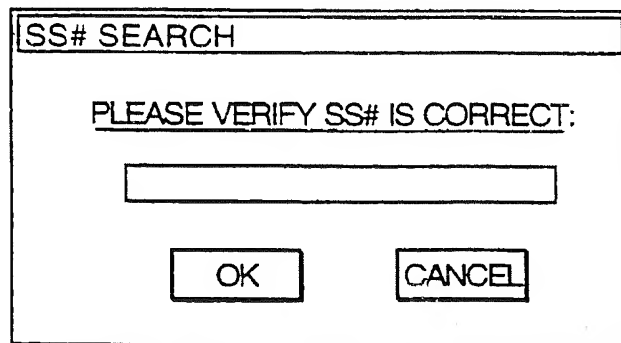
FIG. 11H

19/82



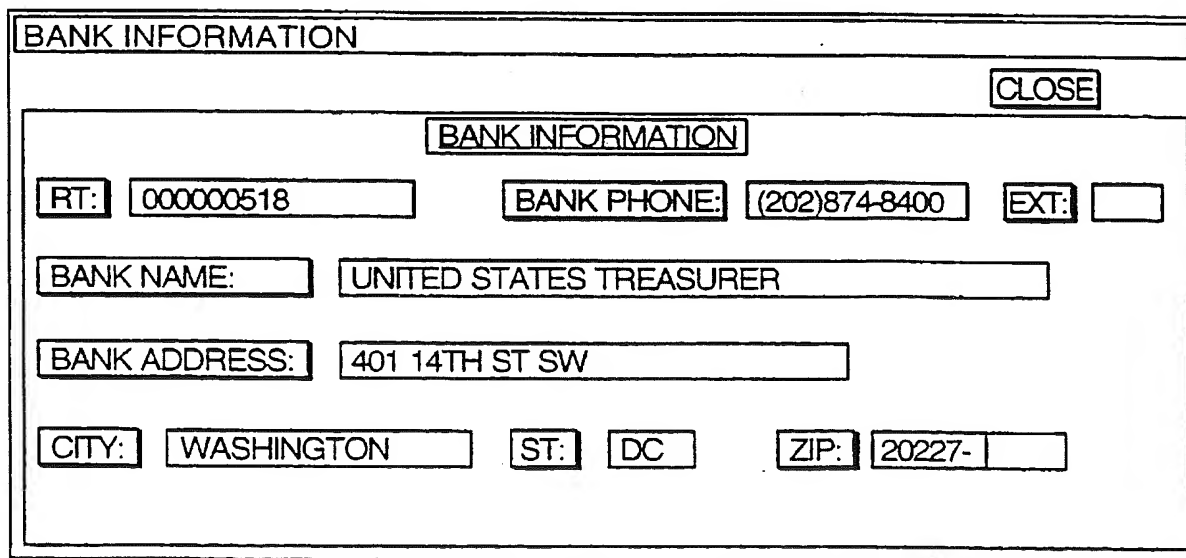
A rectangular dialog box with a title bar that reads "BANK ROUTING NUMBER SEARCH". Below the title bar, the text "PLEASE VERIFY BANK ROUTING NUMBER IS CORRECT:" is displayed. Underneath this text is a single-line text input field. At the bottom of the dialog box are two buttons: "OK" on the left and "CANCEL" on the right.

FIG. 11I



A rectangular dialog box with a title bar that reads "SS# SEARCH". Below the title bar, the text "PLEASE VERIFY SS# IS CORRECT:" is displayed. Underneath this text is a single-line text input field. At the bottom of the dialog box are two buttons: "OK" on the left and "CANCEL" on the right.

FIG. 11J



A rectangular form titled "BANK INFORMATION" in the top-left corner. In the top-right corner of the form is a "CLOSE" button. The form contains several labeled input fields arranged in rows. The first row contains "RT:" followed by a text box with "000000518", "BANK PHONE:" followed by a text box with "(202)874-8400", and "EXT:" followed by an empty text box. The second row contains "BANK NAME:" followed by a text box with "UNITED STATES TREASURER". The third row contains "BANK ADDRESS:" followed by a text box with "401 14TH ST SW". The fourth row contains "CITY:" followed by a text box with "WASHINGTON", "ST:" followed by a text box with "DC", and "ZIP:" followed by a text box with "20227-".

FIG. 11K



TRANSACTION MAINTENANCE

CLOSE

TRANSACTION MAINTENANCE

STORE\_ID:

RT#:  ACCT#:  CHECK#:

AMOUNT:  SS#:

FEE%:

FEE:

PAYBACK:

FIG. 11L

ACTION MAINTENANCE

SAVE CLOSE

ACTION MAINTENANCE

ACTION NUMBER:

DESCRIPTION:

FIG. 11M

SS# SEARCH RESULTS							
SOCIAL SECURITY SEARCH RESULTS						NEW SEARCH	
NAME:			DOB:			CLOSE	
STREET ADDR:			DATE ADDR UPDATED:				
CITY:		ST:		ZIP:		PHONE NUMBER:	
SECOND STREET ADDR:			DATE ADDR UPDATED:				
SECOND CITY:		SECOND ST:		SECOND ZIP:			
THIRD STREET ADDR:			DATE ADDR UPDATED:				
THIRD CITY:		THIRD ST:		THIRD ZIP:			

REFERRAL MAINTENANCE		SAVE		CLOSE	
REFERRAL MAINTENANCE					
REFERRAL NUMBER:	01				
DESCRIPTION:					
NEW PAYOR					
ACTION NUMBER:	01				
STATUS:	M				

FIG. 11N

☐ PAYEE HISTORY SEARCH

PLEASE TYPE IN THE DATE OF TRANSACTION:

▲

▼

◀

▶

CANCEL

CLOSE

OK

FIG. 110

☐ PAYER HISTORY SEARCH X

PLEASE TYPE IN THE DATE OF TRANSACTION:

▲

▼

CANCEL

CLOSE

OK

◀

▶

FIG. 11P

ACTIONS	
<p>CHOOSE PAYOR MAINTENANCE BUTTON, ENROLL, EDIT OR VIEW PAYOR INFORMATION</p> <p>PAYOR MAINTENANCE</p>	<p>CHOOSE PAYEE MAINTENANCE BUTTON, ENROLL, EDIT OR VIEW PAYOR INFORMATION</p> <p>PAYEE MAINTENANCE</p>
<p>CHOOSE CHECK SS# BUTTON, ACCEPT EXISTING INFORMATION, OR PERFORM NEW SEARCH, VERIFY ADDRESS HISTORY, DOB, AND PHONE NUMBER</p> <p>CHECK SS#</p>	<p>CHOOSE VERIFY FUNDS BUTTON, VERIFY ROUTING NUMBER, VIEW BANK INFORMATION, CALL BANK</p> <p>VERIFY FUNDS</p>
<p>CHOOSE PAYOR HISTORY BUTTON, VIEW LIST OF PAST PAYOR TRANSACTIONS</p> <p>PAYOR HISTORY</p>	<p>CHOOSE PAYEE HISTORY BUTTON, VIEW LIST OF PAST PAYEE TRANSACTIONS</p> <p>PAYEE HISTORY</p>
<p>CHOOSE CALL MAKER BUTTON, VERIFY ANY INFORMATION REQUIRED, CALL MAKER</p> <p>CALL MAKER</p>	<p>CHOOSE TRANSACTION MAINTENANCE BUTTON, EDIT OR VIEW INFORMATION</p> <p>TRANSACTION MAINTENANCE</p>

FIG. 11Q

ACTIONS	
<p>CHOOSE SUPERVISOR APPROVAL BUTTON. ALLOW ENTRY OF SUPER- VISOR CODE TO APPROVE ACTION REQUESTED</p> <p>SUPERVISOR APPROVAL</p>	<p>REVIEW PAYEE PICTURES AND COMPARE THEM, IF THEY DO NOT MATCH, YOU MAY RETAKE PICTURE OR REJECT THE TRANSACTION</p> <p>CHECK ID</p>
<p>REVIEW CHECK IMAGE FOR INFORMATION NEEDED, IF ANY INFORMATION IS INCORRECT YOU MAY CALL THE CUSTOMER OR REJECT THE TRANSACTION</p> <p>VERIFY CHECK</p>	<p>REVIEW BACK OF CHECK FOR ENDORSEMENT, IF NOT PRESENT YOU MAY CALL THE CUSTOMER AND REJECT THE TRANSACTION</p> <p>CHECK ENDORSEMENT</p>
<p>CHOOSE RETAKE PICTURE BUTTON, VERIFY IF PICTURE IS GOOD, IF NOT GOOD, REJECT THE TRANSACTION</p> <p>RETAKE PICTURE</p>	<p>CHOOSE CALL CUSTOMER BUTTON, PICK UP THE PHONE</p> <p>CALL CUSTOMER</p>
<p>CHOOSE ACCEPT BUTTON TO ACCEPT THE TRANSACTION</p> <p>ACCEPT</p>	<p>CHOOSE REJECT BUTTON TO REJECT THE TRANSACTION</p> <p>REJECT</p>

FIG. 11R

## REFERRALS

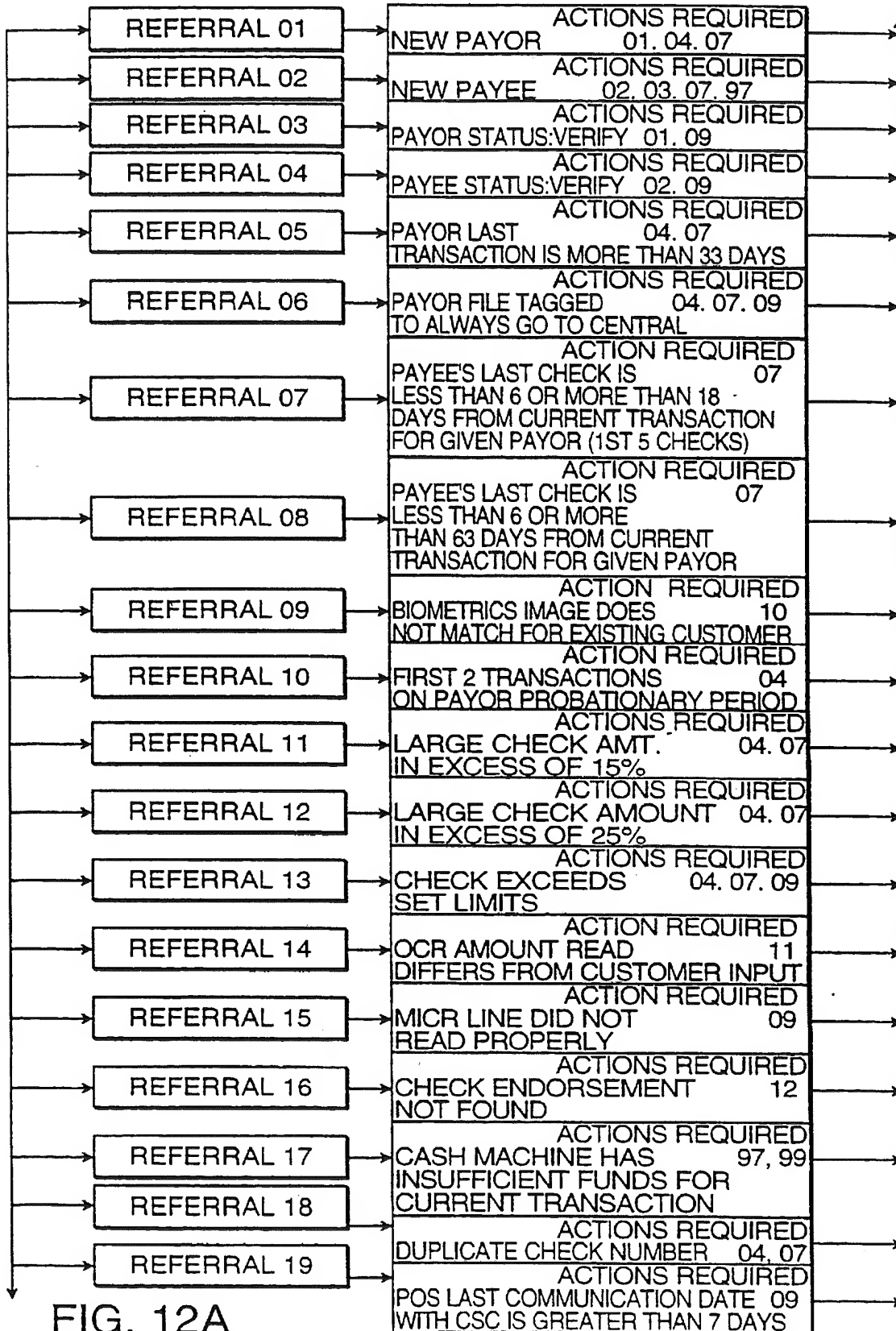


FIG. 12A

## ACTIONS

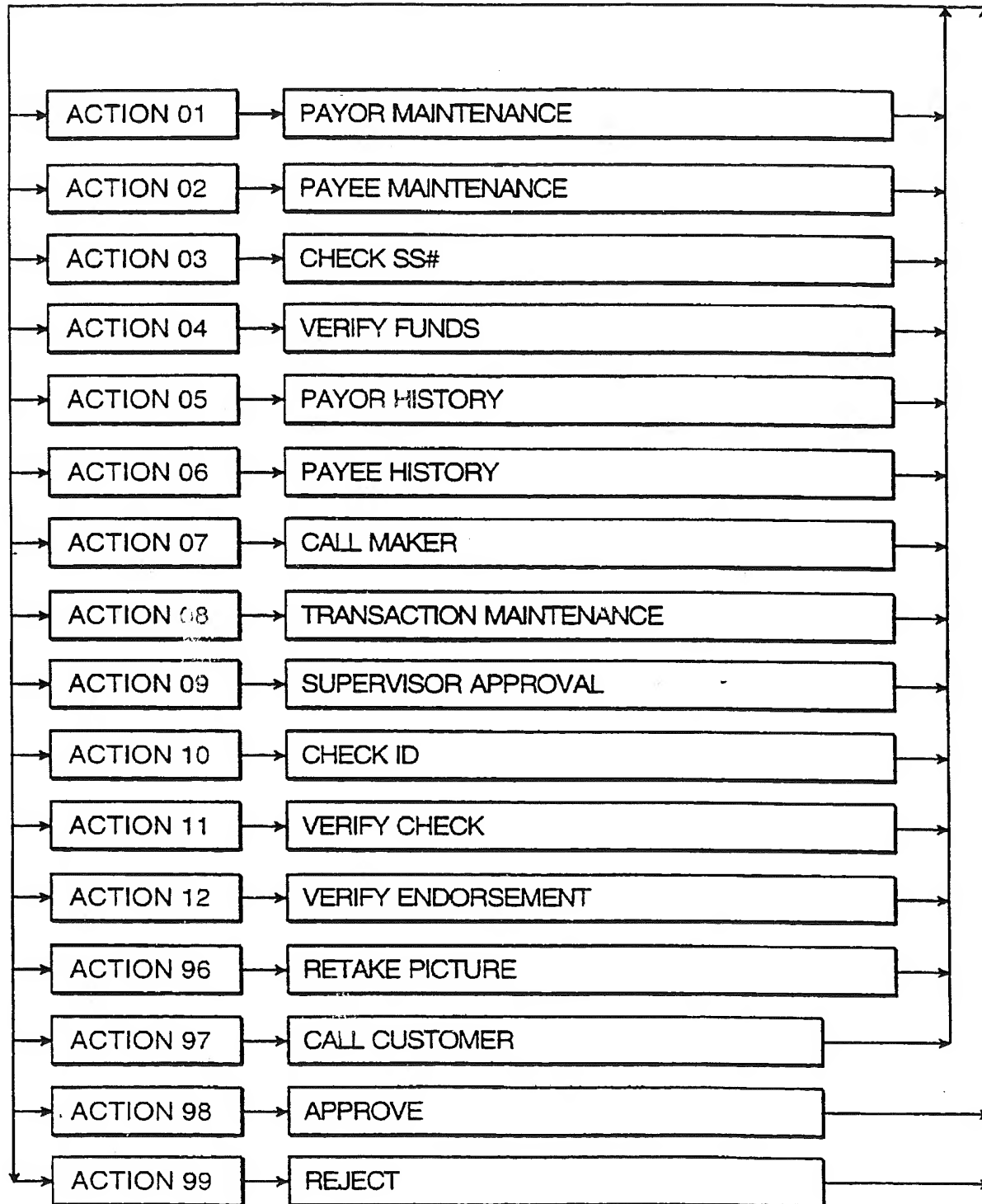


FIG. 12B



## REFERRAL 01 - NEW PAYOR

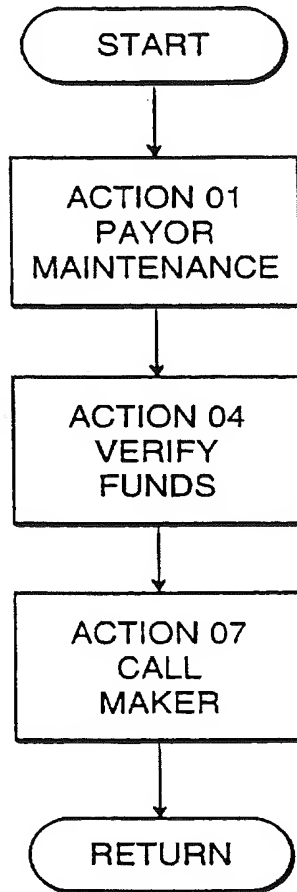


FIG. 13A

## REFERRAL 02 - NEW PAYEE

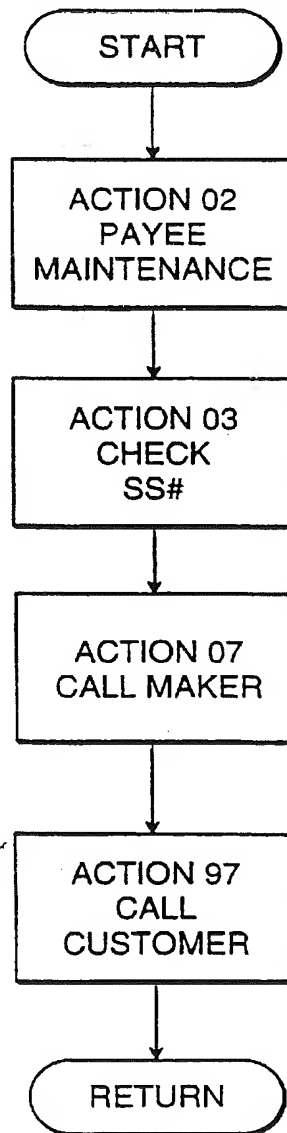


FIG. 13B

## REFERRAL 03 - PAYOR STATUS: VERIFY

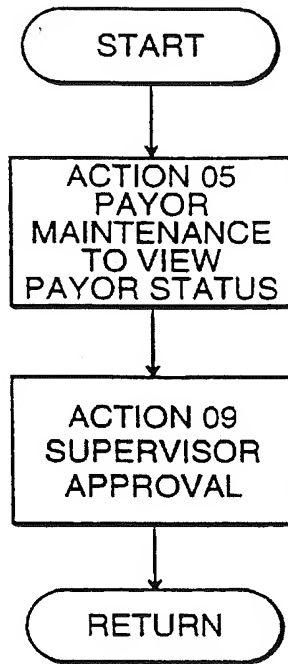


FIG. 13C

## REFERRAL 04 - PAYEE STATUS: VERIFY

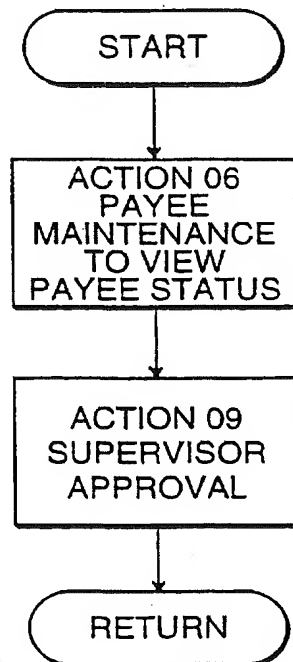


FIG. 13D

REFERRAL 05 - PAYOR LAST TRANSACTION DATE  
IS MORE THAN 33 DAYS

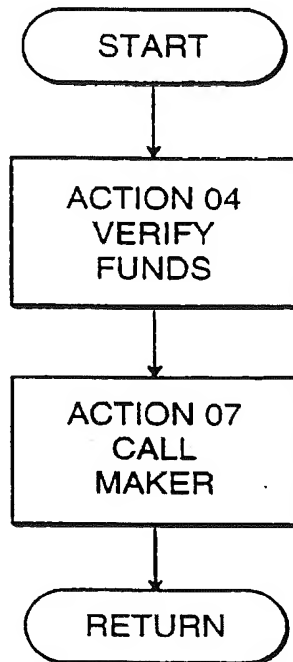


FIG. 13E

REFERRAL 06 - PAYOR FILE TAGGED TO ALWAYS  
GO TO CENTRAL

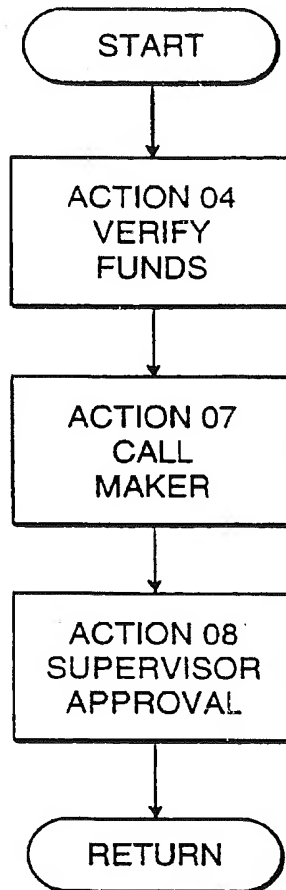


FIG. 13F

REFERRAL 07 - PAYEE'S LAST CHECK IS LESS THAN 6  
OR MORE THAN 18 DAYS FROM CURRENT TRANSACTION  
FOR GIVEN PAYOR (1ST 5 CHECKS ONLY)

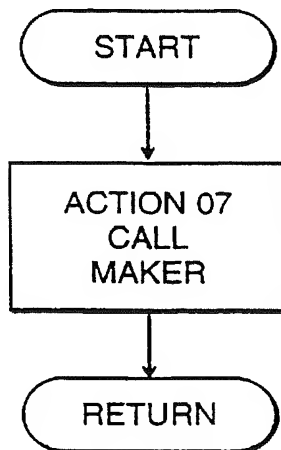


FIG. 13G

REFERRAL 08 - PAYEE'S LAST CHECK IS LESS THAN 6  
OR MORE THAN 63 DAYS FROM CURRENT TRANSACTION  
FOR GIVEN PAYOR

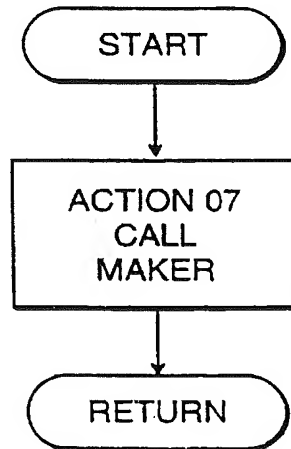


FIG. 13H



REFERRAL 09 - PAYEE'S BIOMETRICS IMAGE DOES  
NOT MATCH FOR EXISTING CUSTOMER

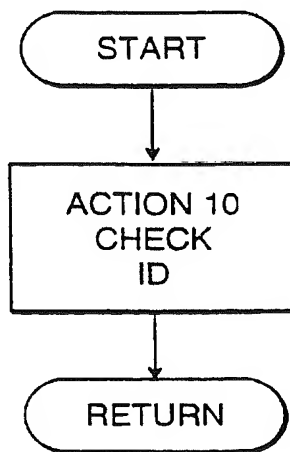


FIG. 13I

REFERRAL 10 - FIRST 2 TRANSACTION ON  
PAYOR PROBATIONARY PERIOD

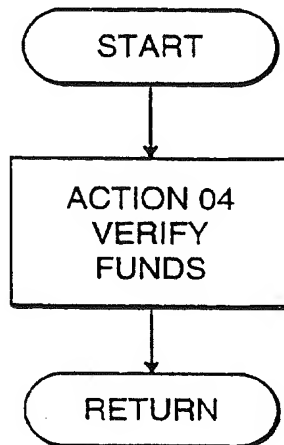


FIG. 13J

## REFERRAL 11 - LARGE CHECK AMOUNT IN EXCESS 15%

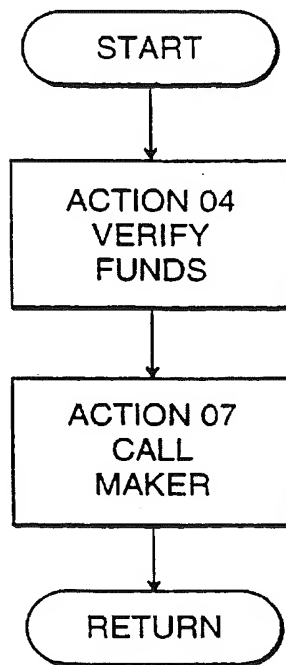


FIG. 13K

## REFERRAL 12 - LARGE CHECK AMOUNT IN EXCESS OF 25%

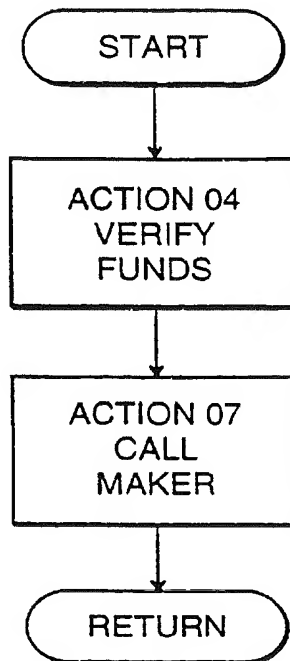


FIG. 13L

## REFERRAL 13 - CHECK EXCEEDS SET LIMITS

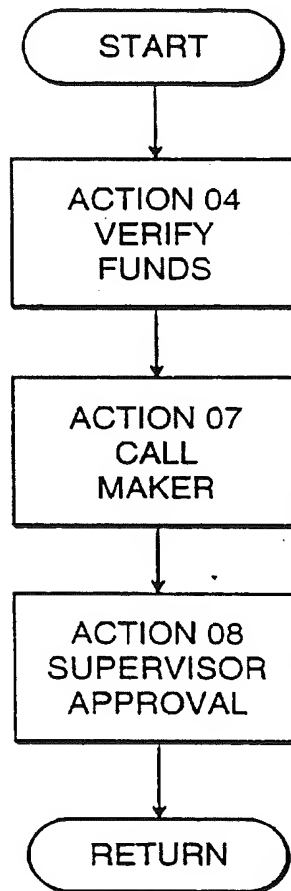


FIG. 13M

REFERRAL 14 - OCR AMOUNT READ DIFFERS  
FROM CUSTOMER INPUT

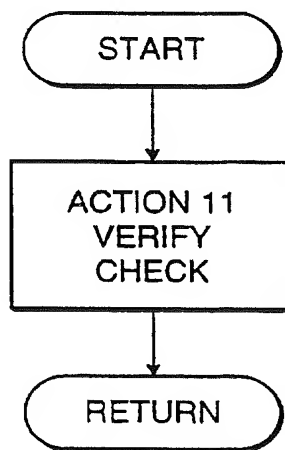


FIG. 13N

## REFERRAL 15 - MICR LINE DID NOT READ PROPERLY

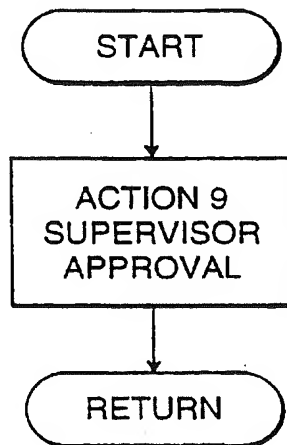


FIG. 130

## REFERRAL 16 - CHECK ENDORSEMENT NOT FOUND

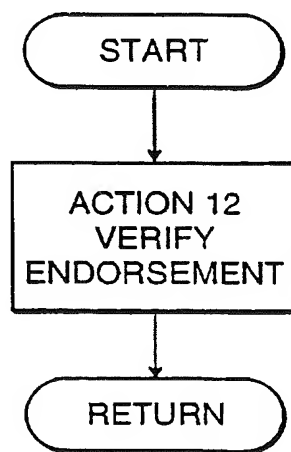


FIG. 13P



## REFERRAL 17 - CASH MACHINE HAS INSUFFICIENT FUNDS

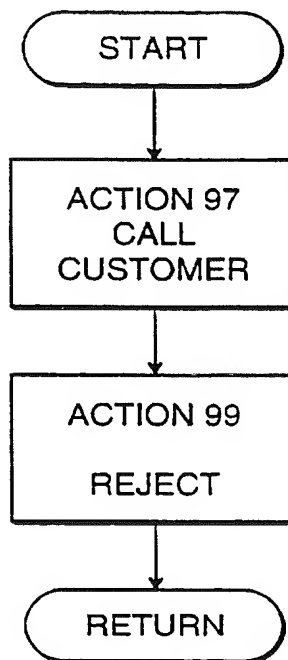


FIG. 13Q

## REFERRAL 18 - DUPLICATE CHECK NUMBER

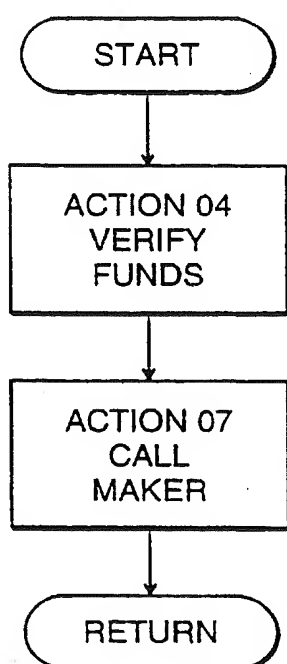


FIG. 13R

REFERRAL 19 - POS LAST COMMUNICATION DATE  
WITH CSC IS GREATER THAN 7 DAYS

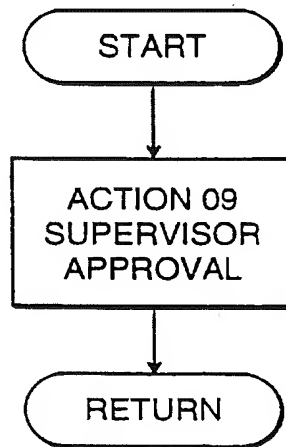


FIG. 13S

## ACTION 01 - PAYOR MAINTENANCE

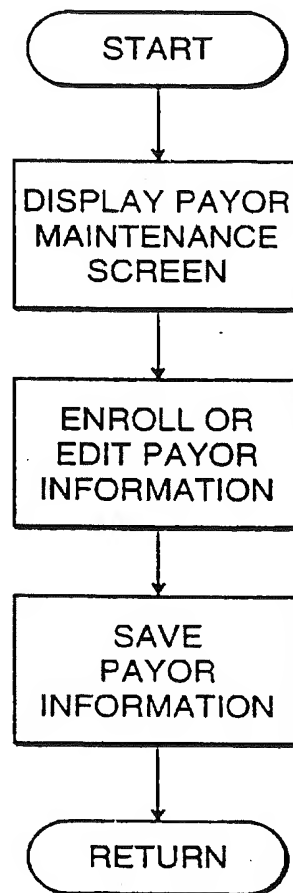


FIG. 14A

## ACTION 02 - PAYEE MAINTENANCE

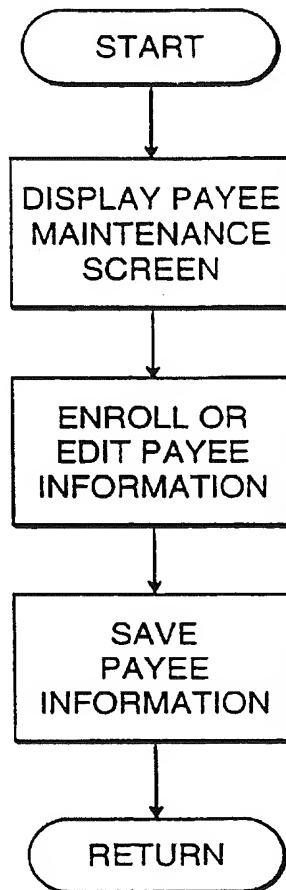


FIG. 14B

## ACTION 03 - CHECK SS#

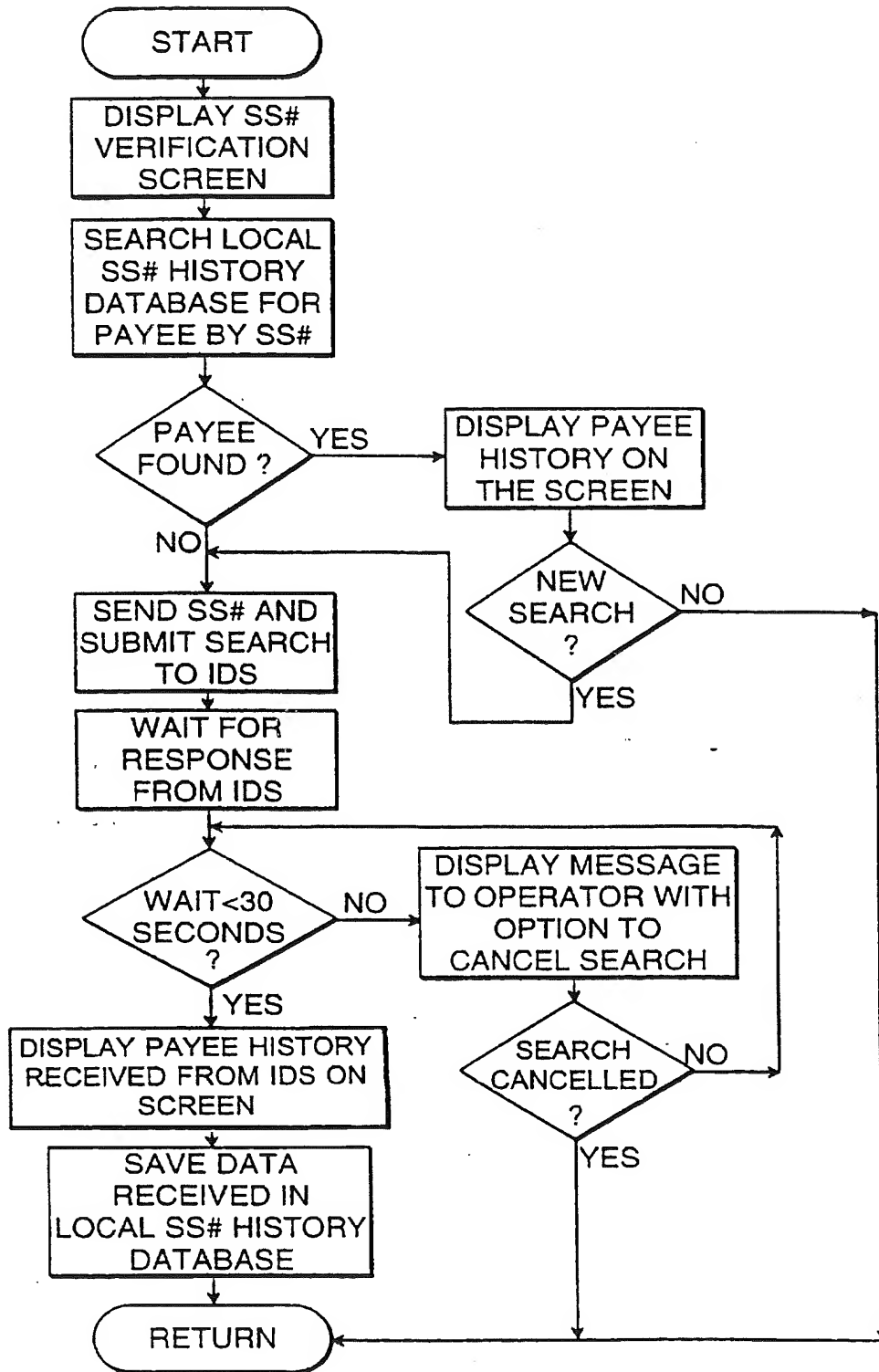


FIG. 14C

## ACTION 04 - VERIFY FUNDS

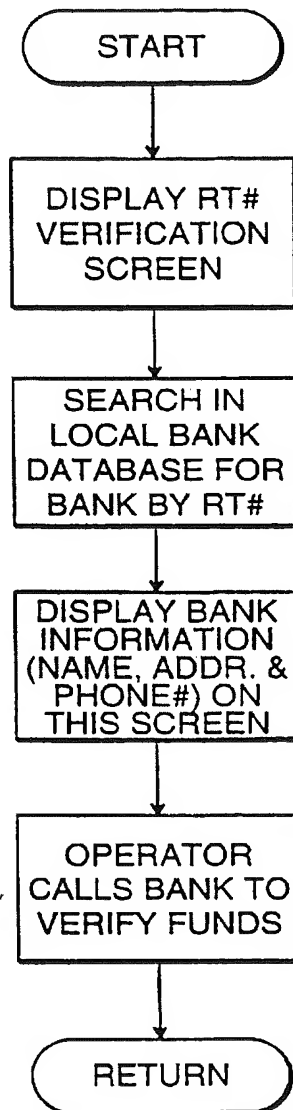


FIG. 14D

## ACTION 05 - PAYOR HISTORY

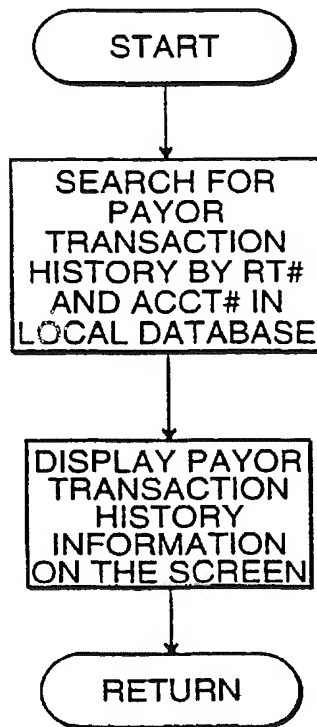


FIG. 14E



## ACTION 06 - PAYEE HISTORY

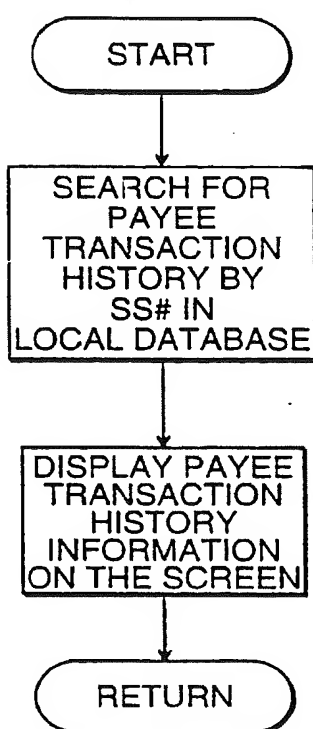


FIG. 14F

## ACTION 07 - CALL MAKER

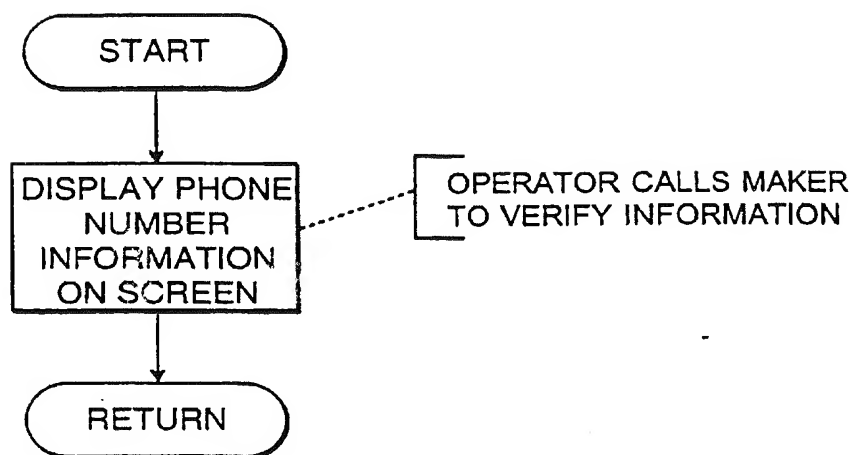


FIG. 14G

## ACTION 08 - TRANSACTION MAINTENANCE

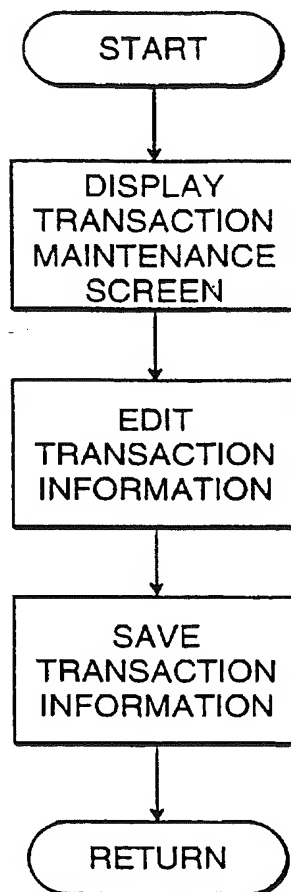


FIG. 14H

## ACTION 08 - SUPERVISOR APPROVAL

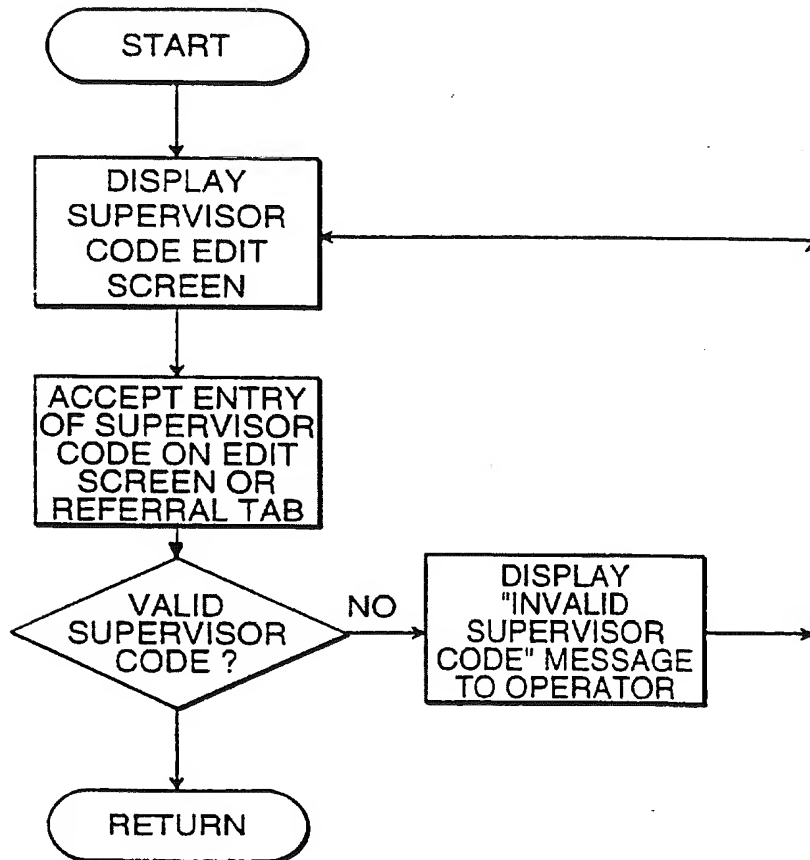


FIG. 14I

## ACTION 10 - CHECK ID

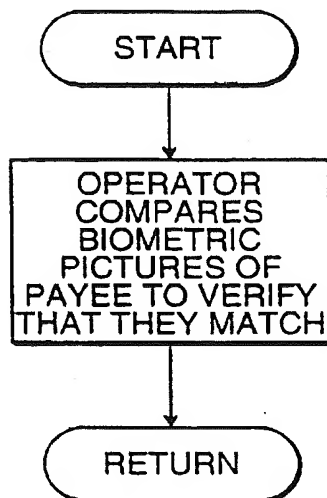


FIG. 14J

## ACTION 11 - VERIFY CHECK

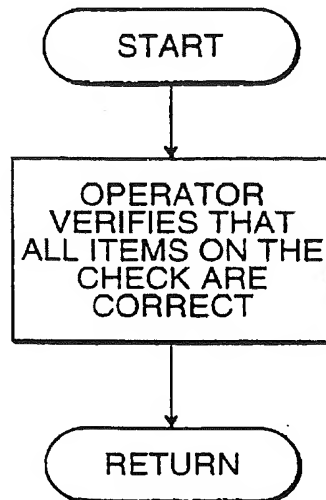


FIG. 14K

## ACTION 12 - VERIFY ENDORSEMENT

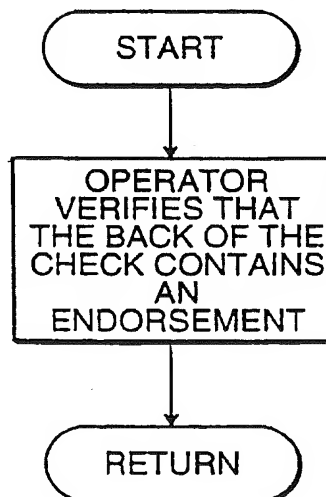


FIG. 14L

## ACTION 96 - RETAKE PICTURE

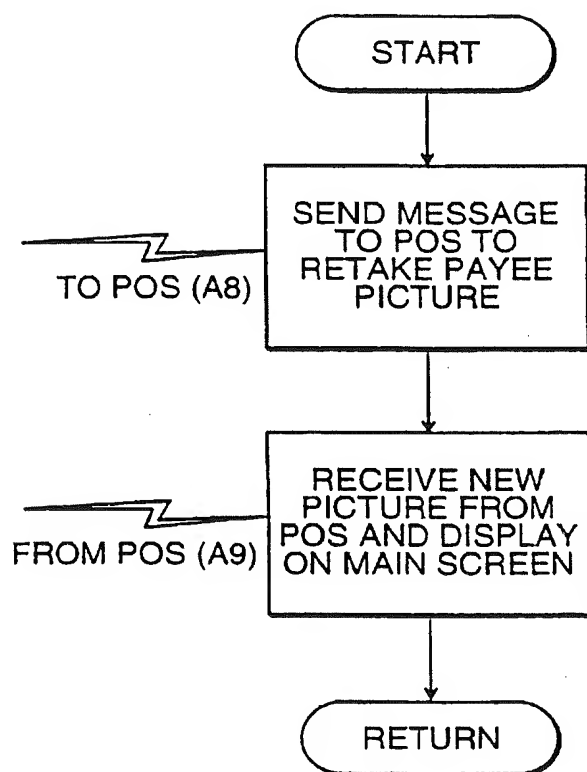


FIG. 14M

## ACTION 97 - CALL CUSTOMER

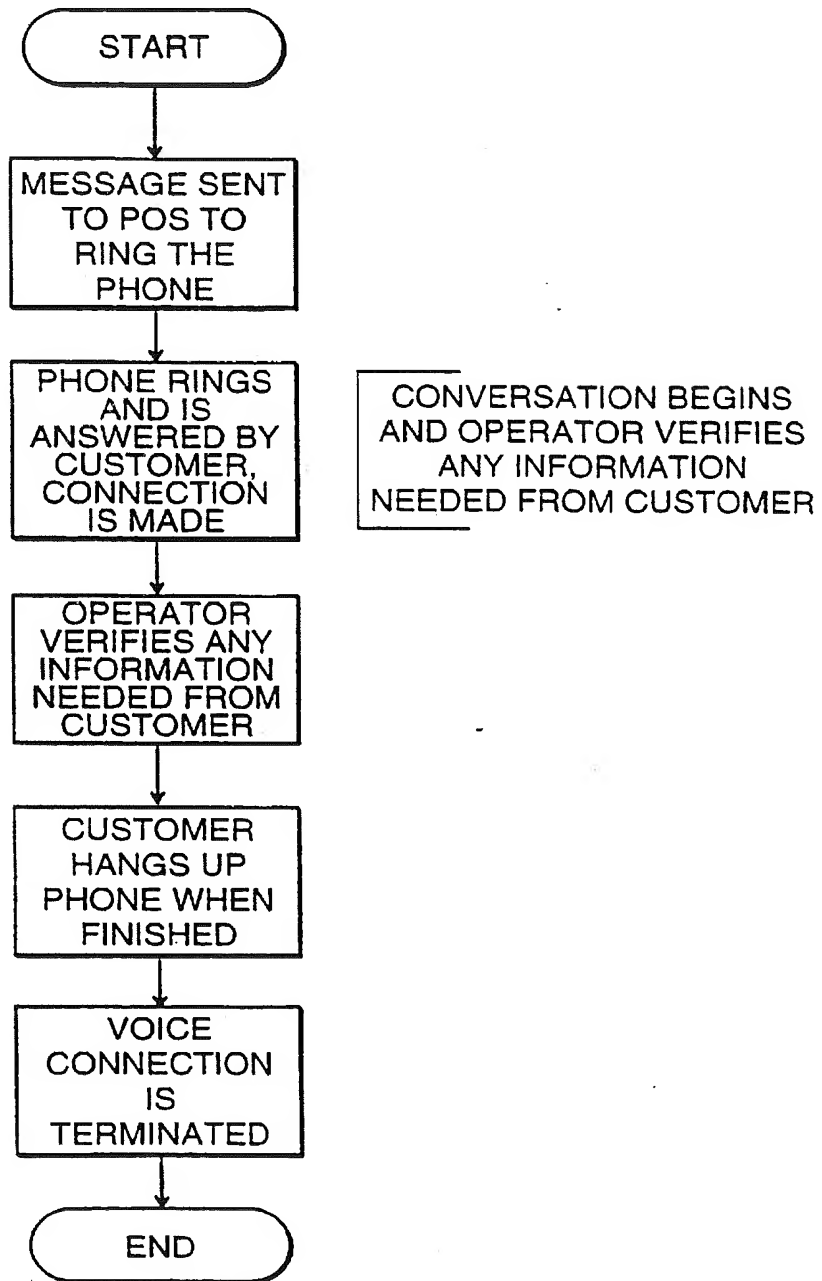


FIG. 14N



## ACTION 98 - APPROVE

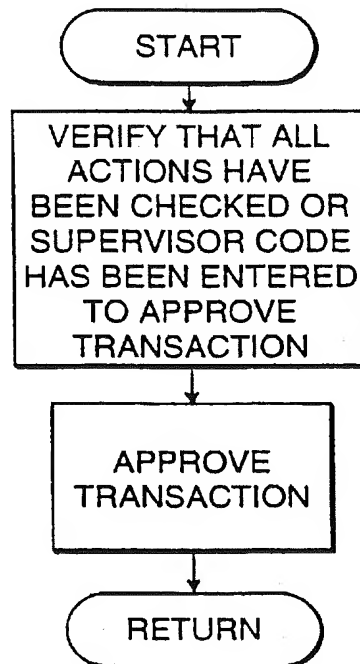


FIG. 140

## ACTION 99 - REJECT

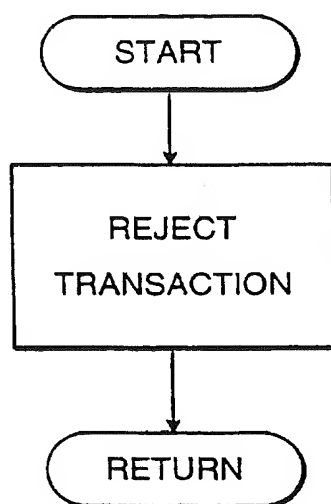


FIG. 14P

## SHARED TABLES

TABLE CHTYPE	FIELD	TYPE	LEN	KEY	SECONDARY INDEXES
MINFEE	CHECKTYPE	ALPHA	1	*	
	FEE%	NUMERIC	4.2		
	DESC	ALPHA	30		
	LIMIT	NUMERIC	9.2		
	MAX	NUMERIC	7.2	*	
	FEE	NUMERIC	7.2		
	SS#	ALPHA	9	*	FULLNAME(LASTNAME+FIRSTNAME)
	STATUS	ALPHA	1		
	LASTNAME	ALPHA	15		LASTNAME(FIRSTNAME
	FIRSTNAME	ALPHA	15		LNAMEDOB(LASTNAME+DOB
PAYEE	MIDDLENAME	ALPHA	15		LFMNAMEDOB(LASTNAME+FIRSTNAME
	PHONE	ALPHA	20		
	ADDR1	ALPHA	30		
	ADDR2	ALPHA	30		
	CITY	ALPHA	15		
	ST	ALPHA	2		
	ZIP	ALPHA	10		
	DOB	DATE			
	SEX	ALPHA	1		
	LASTUPDATEDATE	DATE			
PAYEEID	LASTUPDATETIME	TIME			
	STARTDATE	DATE			
	SS#	ALPHA	9	*	ID# (ID#)
	ID#	ALPHA	15	*	
	IDTYPE	ALPHA	3	*	
	IDST	ALPHA	2		

FIG. 15A

PAYOR	RT#	ALPHA	9	*	NAME (NAME)
	ACCT#	ALPHA	20	*	RT_ACCT (RT# +ACCT#)
	STATUS	ALPHA	3		
	FEDID#	ALPHA	20		CITY (CITY)
	NAME	ALPHA	30		ACCT# (ACCT#)
	ADDR1	ALPHA	30		RT# (RT#)
	ADDR2	ALPHA	30		
	CITY	ALPHA	20		
	ST	ALPHA	2		
	ZIP	ALPHA	10		
	PHONE	ALPHA	12		
	LASTUPDATEDATE	DATE			
	LASTUPDATETIME	TIME			
	STARTDATE	DATE			
OPERATOR	CHECKTYPE	ALPHA	1	*	NAME (NAME)
	OPERATORID	ALPHA	10		
	PASSWORD	ALPHA	10		
	NAME	ALPHA	25		
	SECLEV	NUMERIC	2		
	LANGUAGE	ALPHA	1		

FIG. 15B

# NON SHARED TABLES

TABLE	FIELD	TYPE	LEN	KEY	SECONDARY INDEXES
CHECKAUD	STORE_ID	ALPHA	10	*	
	TRANS#	NUMERIC	10	*	
	SSN	ALPHA	9	*	
	RT#	ALPHA	9		SSN
	ACCT#	ALPHA	20		RAC(RT# +ACCT#)
	CHECK#	ALPHA	30		PCRECDATE(DSCENDING)
	CHECKSCAN	ALPHA	80		
	AMOUNT	NUMERIC	10.2		
	FEE	NUMERIC	10.2		
	LANGUAGE	NUMERIC	1		
	OPERATORID	ALPHA	10		
	RETURNED	ALPHA	1		
	MRPR DISP	NUMERIC	2		
	CUSTOMER DISP	NUMERIC	2		
	HARDWARE DISP	NUMERIC	2		
	PCRECDATE	DATE			
	PCRECTIME	TIME			
	CSCCORERECDATE	DATE			
	CSCCORERECTIME	TIME			
	OPERRECDATE	DATE			
	OPERRECTIME	TIME			
	OPERCMPDATE	DATE			
	OPERCMPTIME	TIME			
	ATMCOMPMDATE	DATE			
	ATMCOMPTIME	TIME			

FIG. 15C

CHECK	SUPERVISOR	ALPHA	10	*	
	STOREID	ALPHA	10	*	
	TRANS#	NUMERIC	8	*	RAC (RT# + ACCT#)
	SSN	ALPHA	9	*	
	RT#	ALPHA	9		PCRECDATE(DESCENDING)
	ACCT#	ALPHA	20		SSN
	CHECK#	ALPHA	30		OPERATORID
	CHECKSCAN	ALPHA	80		
	AMOUNT	NUMERIC	10.2		
	FEE	NUMERIC	10.2		
	LANGUAGE	NUMERIC	1		
	OPERATORID	ALPHA	10		
	RETURNED	ALPHA	1		
	MRPR DISP	NUMERIC	2		
	CUSTOMER DISP	NUMERIC	2		
	HARDWARE DISP	NUMERIC	2		
	PCRECDATE	DATE			
	PCRECTIME	TIME			
	CSCCORECRECDATE	DATE			
	CSCCORERECTIME	TIME			
	OPERRECDATE	DATE			
	OPERRECTIME	TIME			
	OPERCMPDATE	DATE			
	OPERCMPIME	TIME			

FIG. 15D

	ATMCOMPDATE	DATE	
	ATMCOMPTIME	TIME	
	SUPERVISOR	ALPHA	10
POSINFO	STORE_ID	ALPHA	10 *
	BDEN1	NUMERIC	4
	BDEN2	NUMERIC	4
	BDEN3	NUMERIC	4
	BDEN4	NUMERIC	4
	CDEN1	NUMERIC	3.2
	CDEN2	NUMERIC	3.2
	CDEN3	NUMERIC	3.2
	CDEN4	NUMERIC	3.2
	LASTCOMMPOSDATE	DATE	
	LASTCOMMPOSTIME	TIME	
	POSDATAPHONE	ALPHA	10
	POSVOICEPHONE	ALPHA	10
	FIRSTNSFGRACE	NUMERIC	2
CHKREJRSN	STORE_ID	ALPHA	10 *
	TRANS#	NUMERIC	10 *
	RSNCODE	ALPHA	2
REJRSN	RSNCODE	ALPHA	2 *
	RSNDESC	ALPHA	130
CHKREFRL	STOREID	ALPHA	10 *
	TRANS#	NUMERIC	10 *
	REFNUM	ALPHA	2

FIG. 15E

PRYNOTES	RT#	ALPHA	9	*
	ACCT#	ALPHA	20	*
	NOTES	ALPHA	600	
PYENOTES	SSN	ALPHA	9	*
	NOTES	ALPHA	600	
CHKRTN	STOREID	ALPHA	10	*
	TRANS#	NUMERIC	10	*
	SSN	ALPHA	9	*
	RTNDATE	DATE		
	RTNREASON	ALPHA	130	
POSSITES	STOREID	ALPHA	10	*
	ADDR1	ALPHA	30	
	ADDR2	ALPHA	30	
	CITY	ALPHA	20	
	STATE	ALPHA	2	
SSRSLTS	SSNUM	ALPHA	9	*
	SEQ#	NUMERIC	2	*
	FIRSTNAME	ALPHA	20	
	MIDDLENAME	ALPHA	20	
	LASTNAME	ALPHA	20	
	HOUSENUM	ALPHA	10	
	STREETNAME	ALPHA	20	
	STREETTYPE	ALPHA	10	
	APARTNUM	ALPHA	10	

FIG. 15F



CITY	ALPHA	20
STATE	ALPHA	2
ZIP	ALPHA	9
PHONENUM	ALPHA	10
DOB	ALPHA	8
DATEADDR	DATE	
SECHOUSENUM	ALPHA	6
SECSTNAME	ALPHA	19
SECSTTYPE	ALPHA	2
SECAPARTNUM	A	5
SECCITY	A	16
SECSTATE	A	2
SECZIP	A	9
DATEADDR2	DATE	
THRDHOUSENUM	A	6
THRDSTNAME	A	19
THRDSTTYPE	A	2
THRDAPARTNUM	A	5
THRDCITY	A	16
THRDSTATE	A	2
THRDZIP	A	9
DATEADDR3	DATE	

FIG. 15G

INPUTQUERY	IDENTIFIER	ALPHA	2
	TYPE	ALPHA	3
	LASTNAME	ALPHA	20
	MIDDLENAME	ALPHA	10
	FIRSTNAME	ALPHA	10
	FIRSTNAMETYPE	ALPHA	1
	STREETNUM	ALPHA	7
	PREDIR	ALPHA	2
	NAME	ALPHA	19
	TYPE	ALPHA	2
	APARTNUM	ALPHA	5
	UNUSED	ALPHA	4
	CITY	ALPHA	15
	STATE	ALPHA	2
	ZIP	ALPHA	9
	PHONE	ALPHA	10
	TIESFLAG	ALPHA	1
	SCROLLKEY	ALPHA	6
	CUSTACCT	ALPHA	18
	NAMEPARSEFLG	ALPHA	1
	SSNUM	ALPHA	9
	DRIVERSNUM	ALPHA	27
	DRIVERSTATE	ALPHA	2

FIG. 15H

	STREETPARSEFLG	ALPHA	1	
	DOB	ALPHA	8	
	EMPSEGCOUNT	ALPHA	1	
	PROPSEGCOUNT	ALPHA	1	
	MISCSEGCOUNT	ALPHA	1	
	RESERVED	ALPHA	52	
BANKINFO	ITUPDATE	ALPHA	6	
	INSTTYPE	ALPHA	2	
	RTMICR	ALPHA	9	* RTMICR
	INSTNAME	ALPHA	50	
	STADDR	ALPHA	40	
	CITY	ALPHA	30	
	STABBR	ALPHA	2	
	ZIPCODE	ALPHA	5	
	ZIP4	ALPHA	4	
	AREACODE	ALPHA	3	
	PHONENUM	ALPHA	7	
	PHONEEXT	ALPHA	5	
	Fedresv	ALPHA	6	
ACTIONS	ACTIONNUM	ALPHA	2	*
	DESCRIPTION	ALPHA	130	
	HELPTXT	ALPHA	130	

FIG. 15I

REFERRALS	REFNUM	ALPHA	2	*	
	DESCRIPTION	ALPHA	120		
	ACTIONNUM	ALPHA	2	*	
	STATUS	ALPHA	1		
PYETMPL	SSN	ALPHA	9	*	
	TMPL	BLOB			TMPL
PYETRANSPIC	TRANS#	NUMERIC	10	*	SSN
	BMPFILENAME				
PYEPIC	SSN	ALPHA	9	*	
	BMPFILENAME				
ATMINVBILLS	STOREID	ALPHA	10	*	
	DATE	DATE		*	
	TIME	TIME		*	
	CNT_BILLS_1	NUMERIC	4.0		
	CNT_BILLS_2	NUMERIC	4.0		
	CNT_BILLS_3	NUMERIC	4.0		
	CNT_BILLS_4	NUMERIC	4.0		
	CNT_BILLS_1_REJ	NUMERIC	4.0		
	CNT_BILLS_2_REJ	NUMERIC	4.0		
	CNT_BILLS_3_REJ	NUMERIC	4.0		
	CNT_BILLS_4_REJ	NUMERIC	4.0		

FIG. 15J

72/82

	CNT_BILLS_1_STS	ALPHA	1.0	
	CNT_BILLS_2_STS	ALPHA	1.0	
	CNT_BILLS_3_STS	ALPHA	1.0	
	CNT_BILLS_4_STS	ALPHA	1.0	
ATMINVCOINS	STOREID	ALPHA	10	*
	DATE	DATE		*
	TIME	TIME		*
	CNT_COINS_1	NUMERIC	4.0	
	CNT_COINS_2	NUMERIC	4.0	
	CNT_COINS_3	NUMERIC	4.0	
	CNT_COINS_4	NUMERIC	4.0	
	CNT_COINS_1_STS	ALPHA	1.0	
	CNT_COINS_2_STS	ALPHA	1.0	
	CNT_COINS_3_STS	ALPHA	1.0	
	CNT_COINS_4_STS	ALPHA	1.0	
ATMERRORLOG	STOREID	ALPHA	10	*
(UNSOLICITED)	DATE	DATE		*
	TIME	TIME		*
	MSGTYPE	ALPHA	6	
	MESSAGE	ALPHA	100	
PRNTCHK	TRANS#	NUMERIC	10	*
	BMPFILENAME			

FIG. 15K

BAKCHK	TRANS#	NUMERIC	10	*
	BMPFILENAME			

FIG. 15L

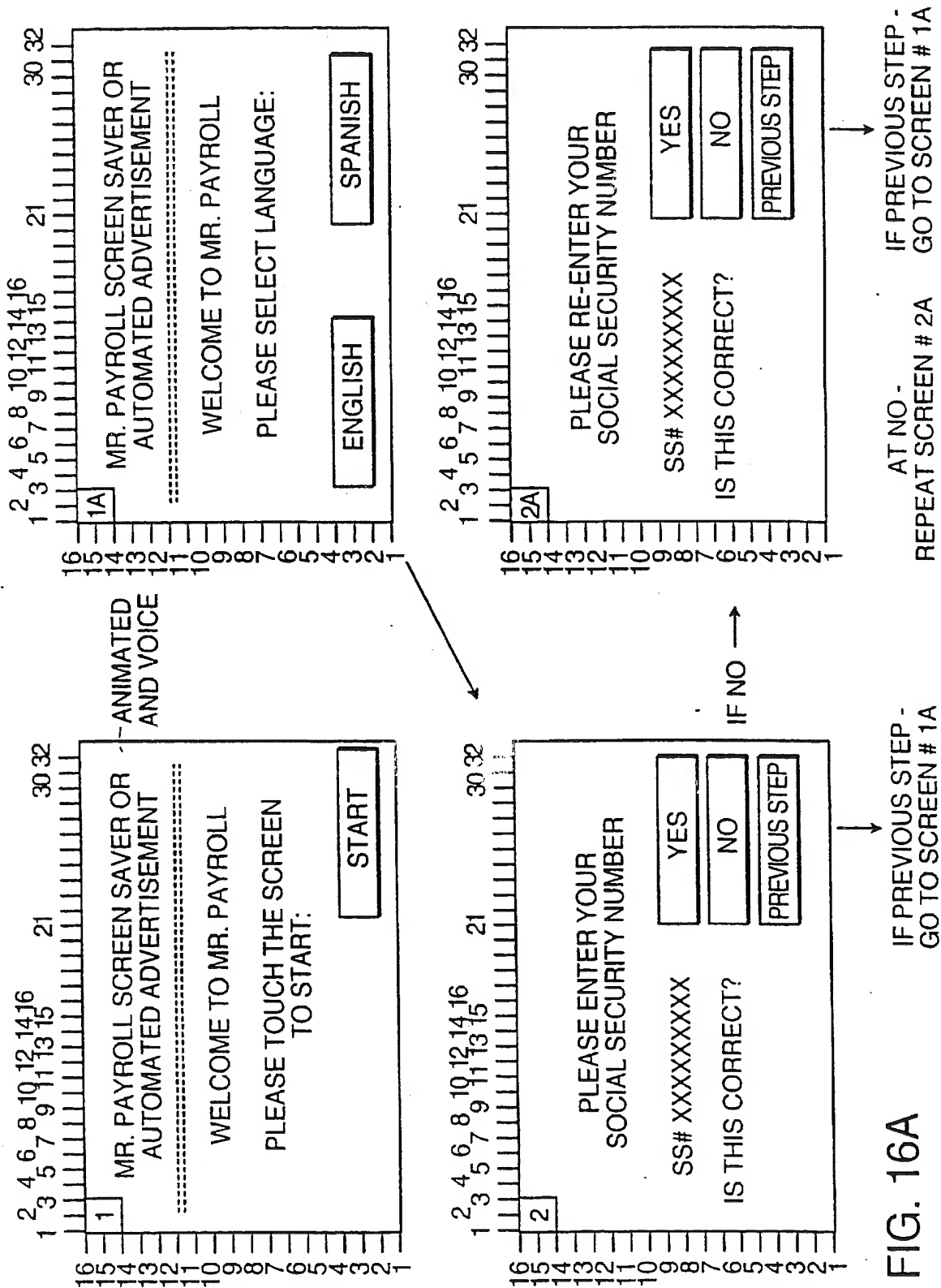


FIG. 16A

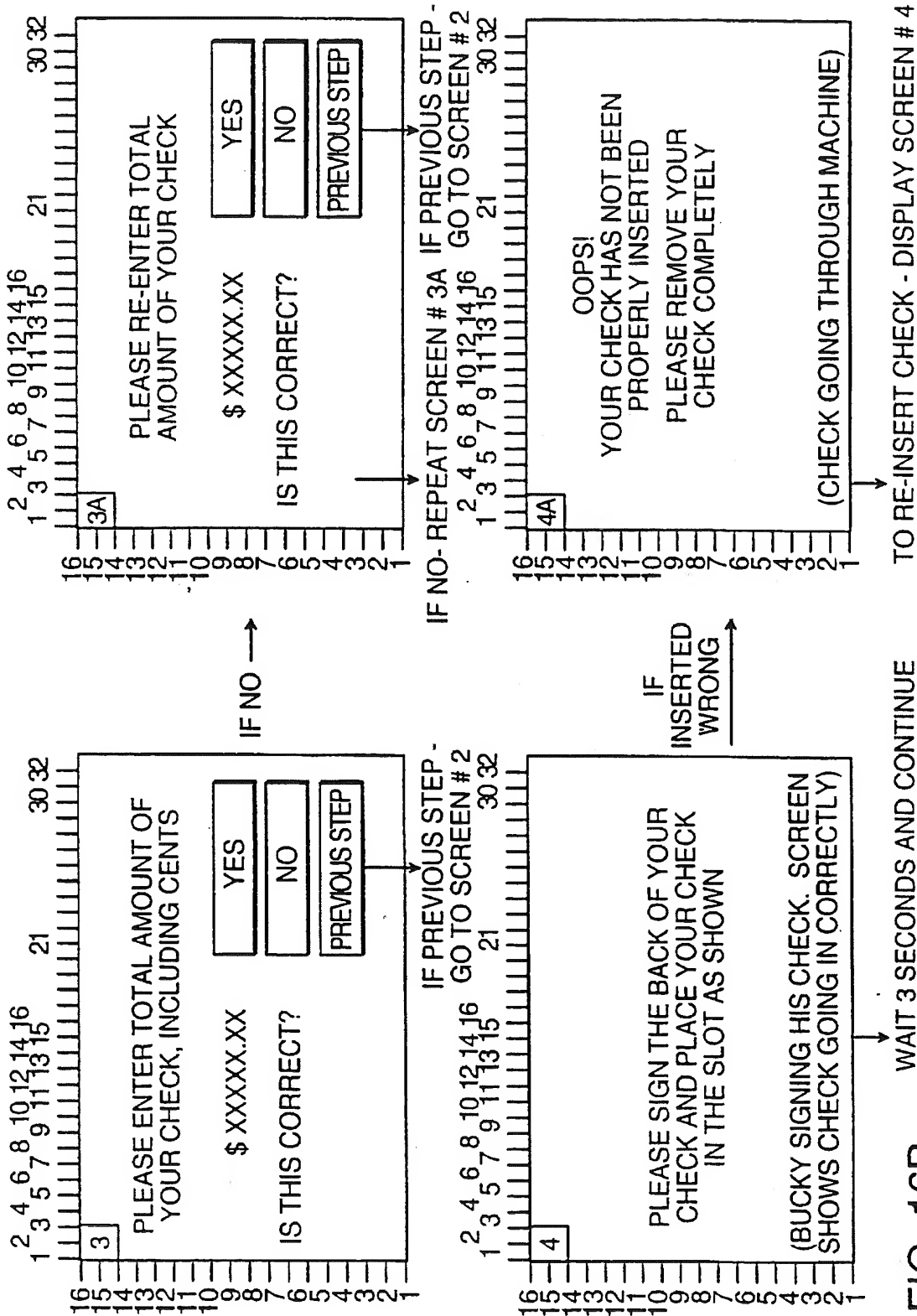


FIG. 16B

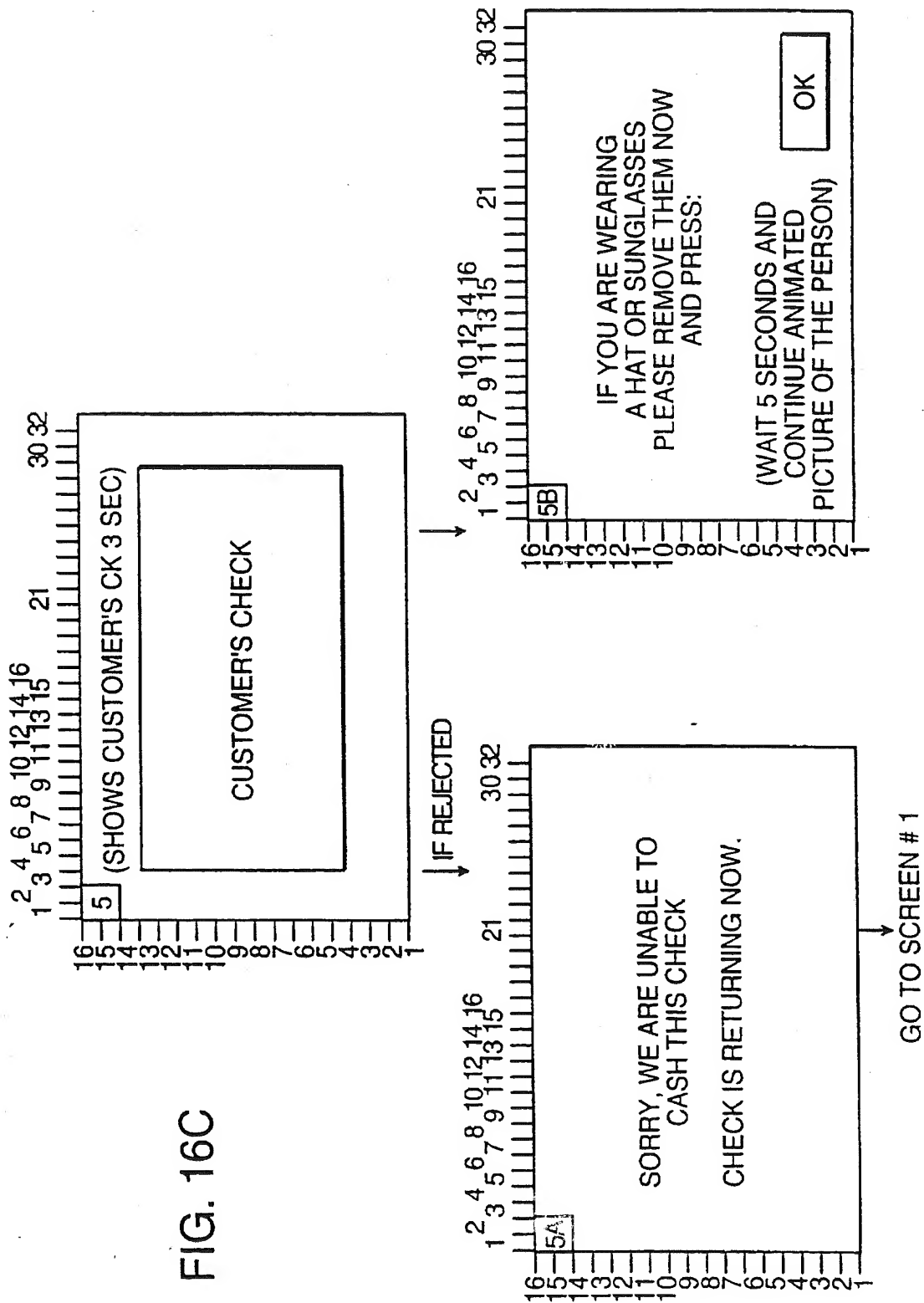


FIG. 16C



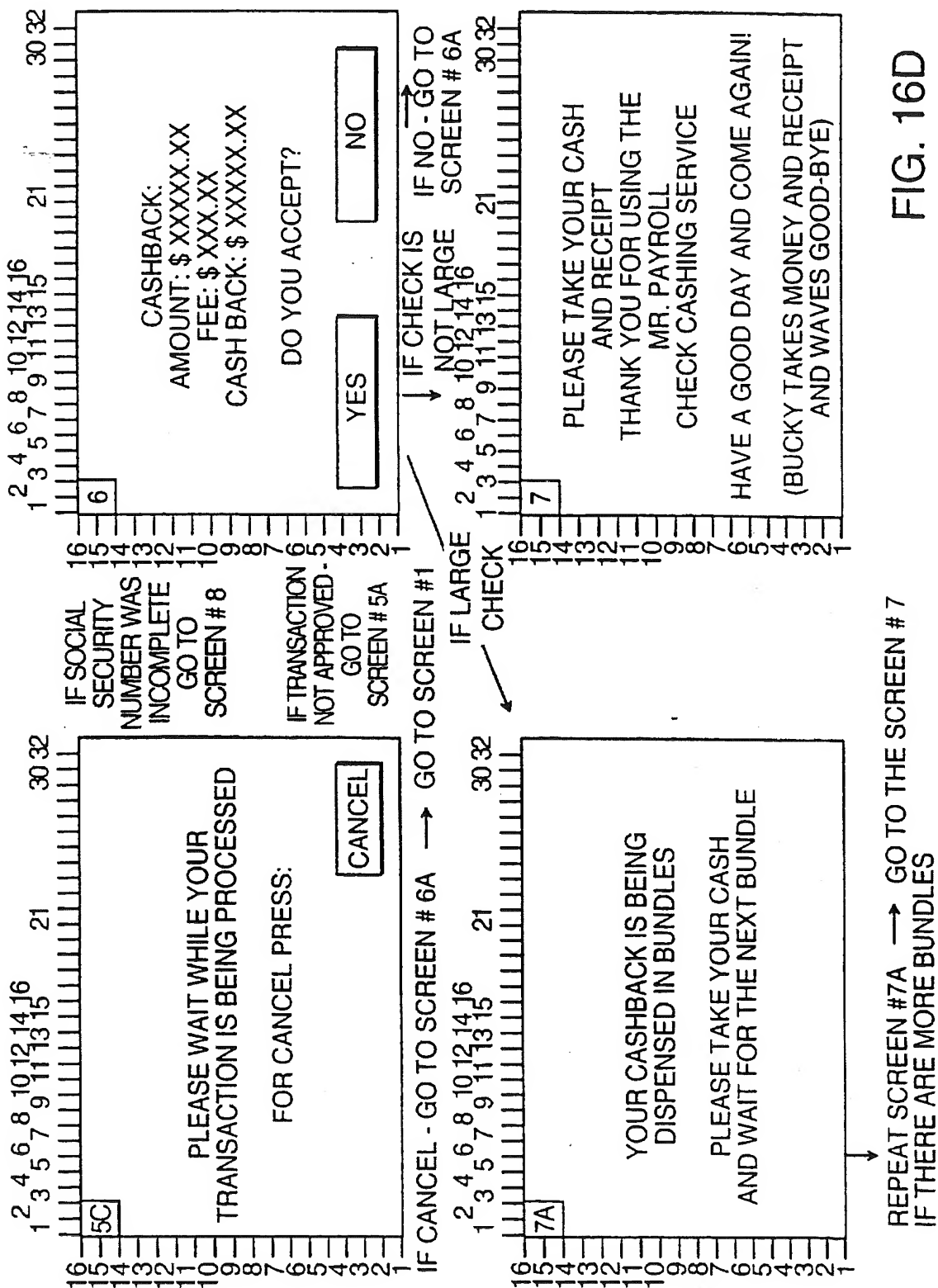


FIG. 16D

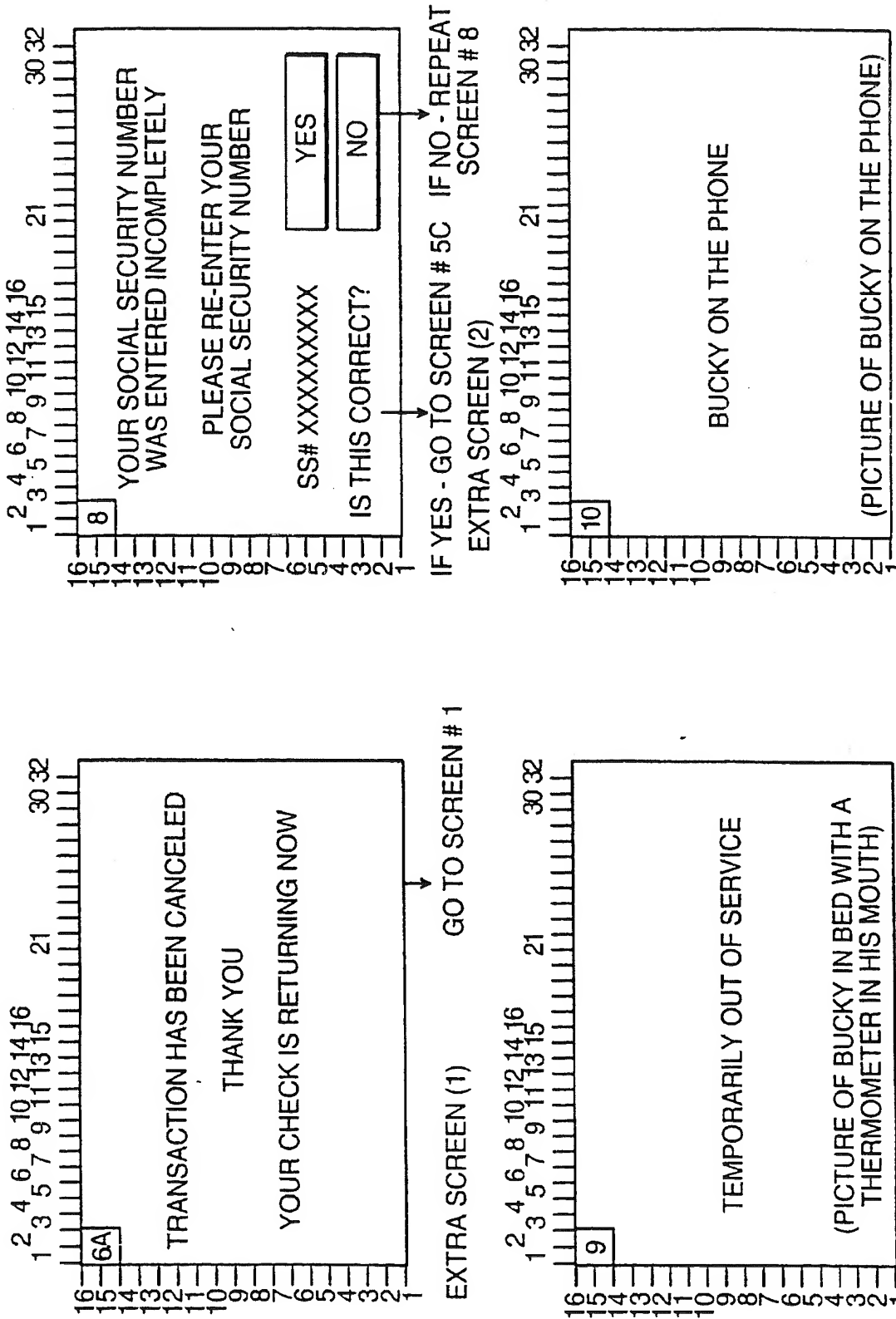
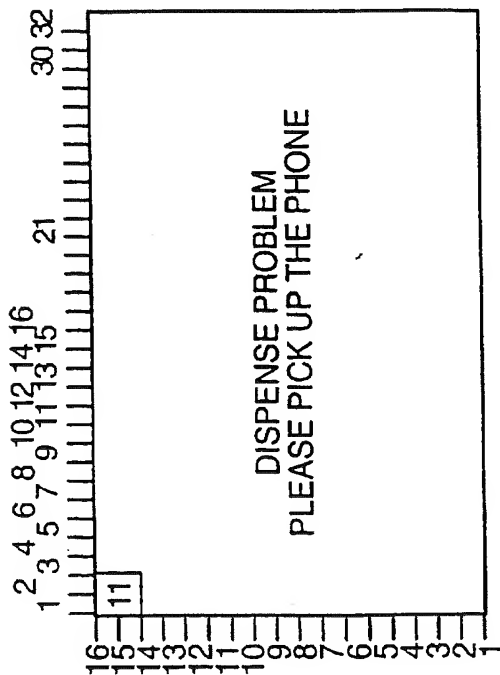
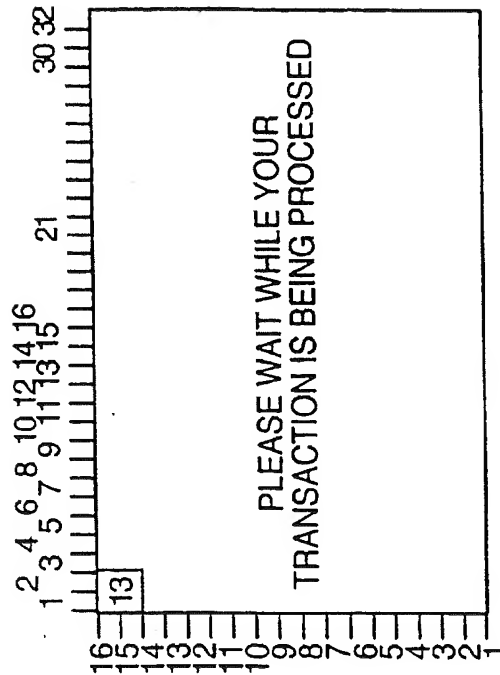


FIG. 16E

EXTRA SCREEN (3)



EXTRA SCREEN (5)



EXTRA SCREEN (4)

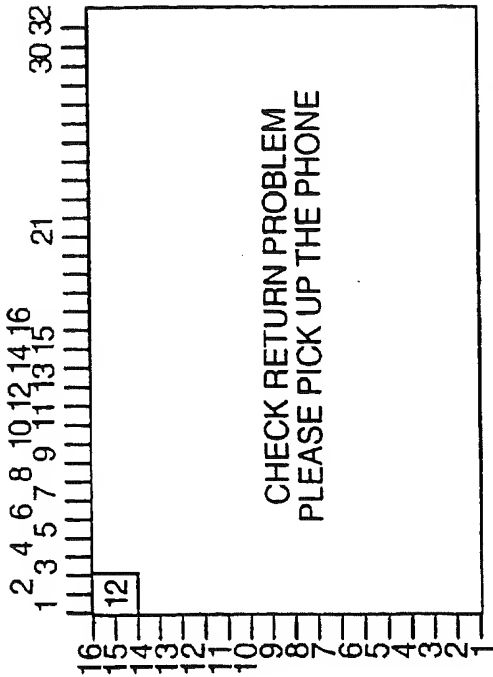


FIG. 16F

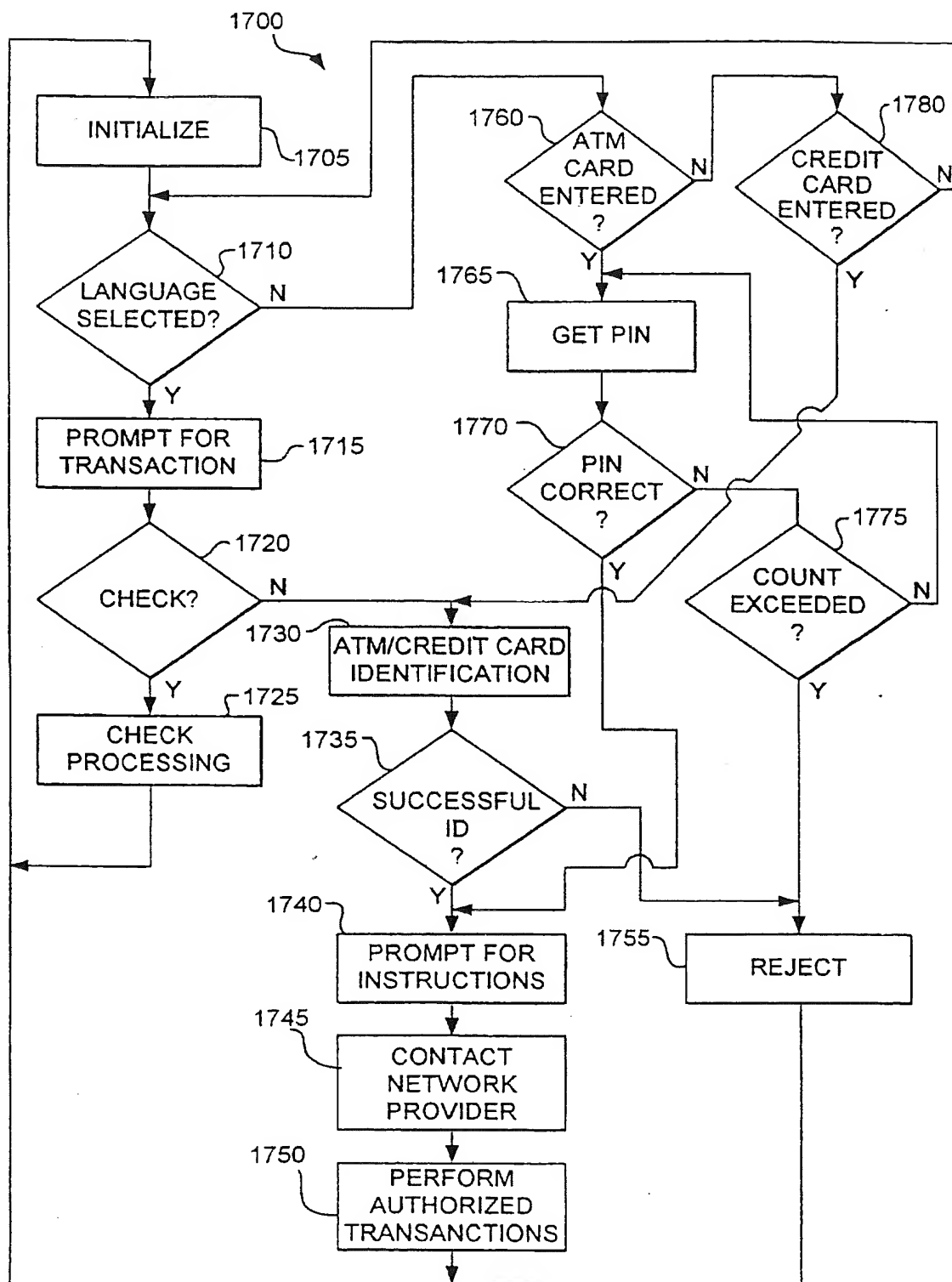


FIG. 17

80/82

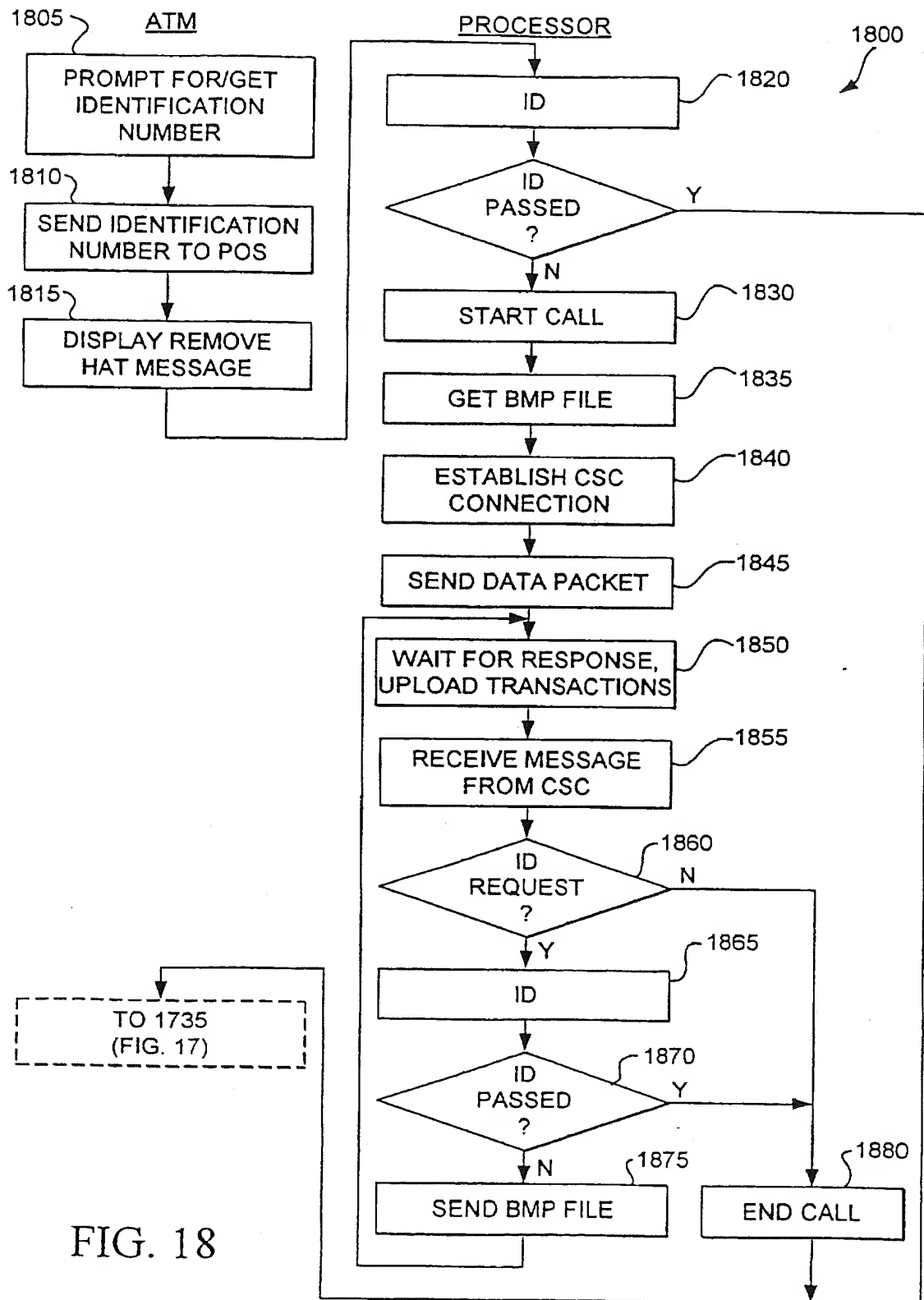


FIG. 18

1900

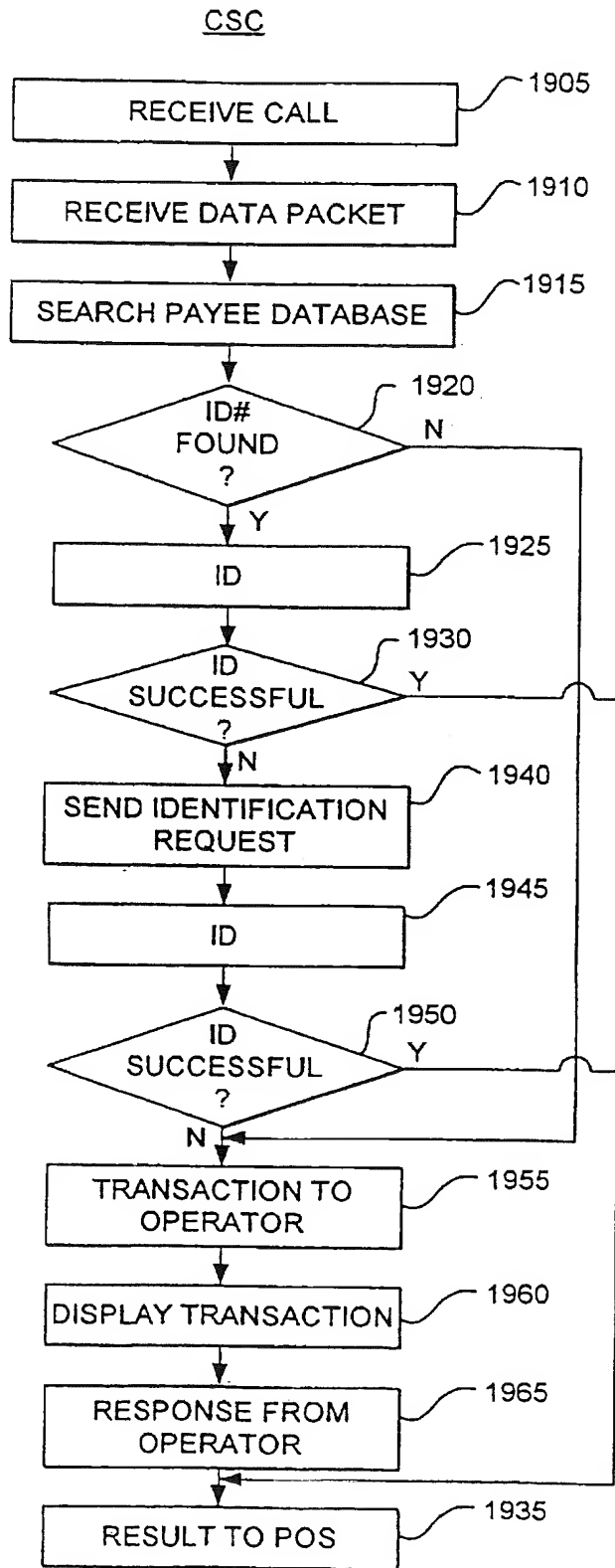


FIG. 19

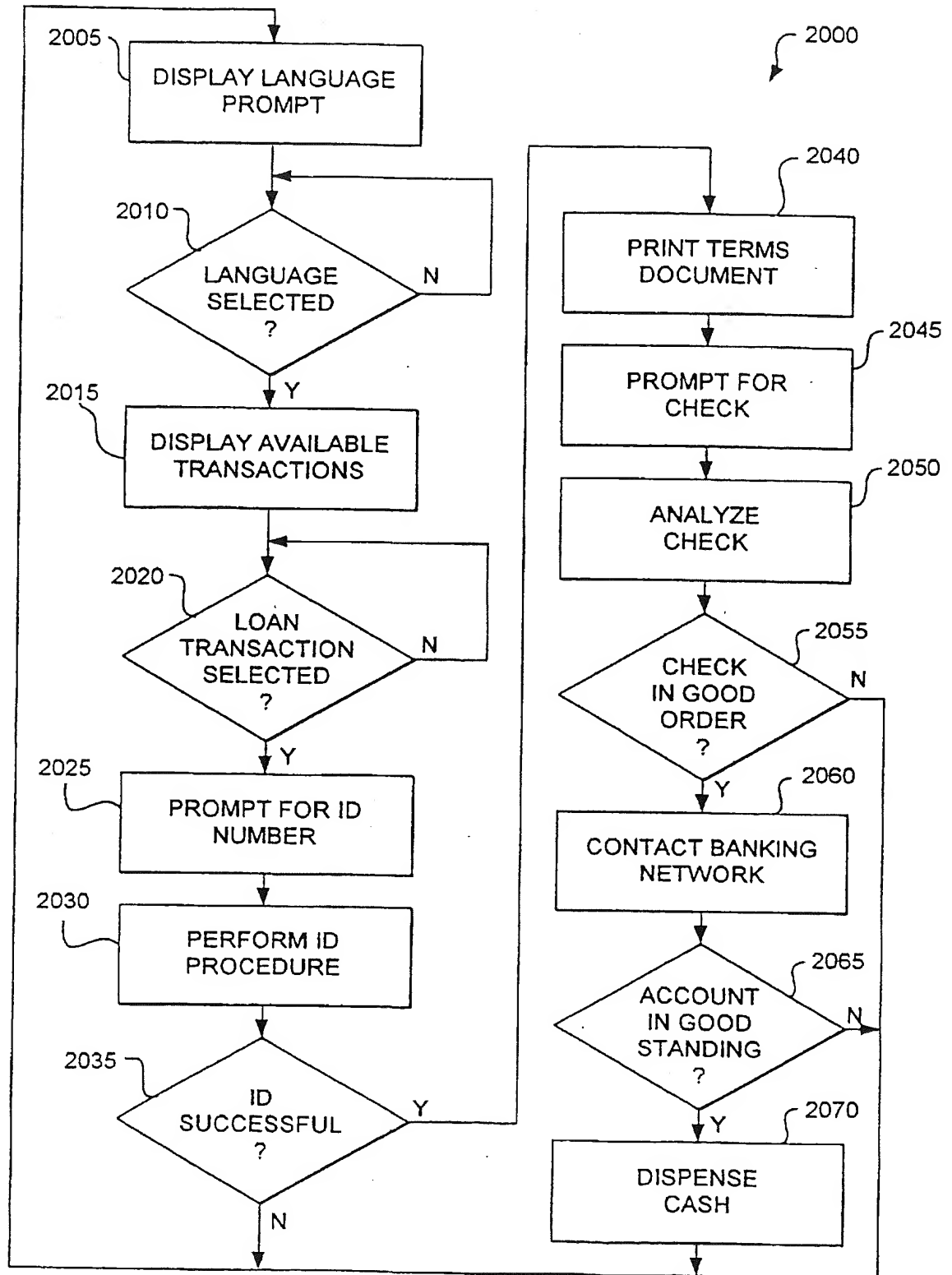


FIG. 20

## PINLESS CASH ADVANCES

5

10

The invention relates to obtaining a cash advance using a credit card or a debit card.

15

In general, a cardholder uses an automated teller machine ("ATM") to obtain a credit card or debit card cash advance. The cardholder inserts the card into a slot of the ATM. The card includes a magnetic strip on which is encoded information about the card account (e.g., the account number). The ATM responds to insertion of the card by prompting the cardholder to enter the cardholder's personal identification number ("PIN"). The ATM then uses the PIN to determine whether the cardholder is actually is authorized to use the card.

20

One aspect of the invention provides credit card or debit card cash advances through unmanned ATMs without requiring the use of a PIN and, in some instances, without requiring the insertion of a credit card or debit card. These transactions are designated, respectively, as pinless cash advances and cardless cash advances. For ease of discussion, the following description refers to credit cards. However, one of skill in

25



the art will recognize that the described systems and techniques also are applicable to debit cards and similar devices. For example, instead of dispensing cash, the described systems and techniques could be used to apply credits to a cash card.

5 The ATMs use biometric information instead of a PIN to confirm the customer's identity. For example, the ATM may produce an image of the customer's face as the customer types in an identification number or inserts a card, and then may compare the image with an image stored in association with the identification number or card number to verify the customer's identity. Use of biometric information promises to vastly improve the identification process and to reduce or eliminate the  
10 occurrence of fraudulent cash advances. In addition, elimination of the need for PINs or cards when obtaining cash advances promises to increase the convenience of obtaining cash advances.

In one aspect, generally, an apparatus for providing pinless, automated cash advances includes an input device configured to generate an input signal corresponding  
15 to a customer identifier in response to actuation of the input device by a customer, a biometric device configured to receive biometric information about the customer, and a storage device including a database of customer information that includes stored biometric information. An electronic processor of the apparatus is configured to receive the input signals from the input device, receive biometric information from the  
20 biometric device, and access the database of customer information to obtain data about the customer, the data including stored biometric information for the customer. The electronic processor then compares the received biometric information to the stored biometric information and contacts a verification network to request authorization for a cash advance. The processor approves the cash advance when the received biometric  
25 information matches the stored biometric information to a degree sufficient to confirm the customer's identity, and upon receiving authorization for the cash advance from the verification network.

Further aspects of the invention are exemplified by the attached claims.

Embodiments may include one or more of the following features. The apparatus may further include a cash dispenser, with the electronic processor being configured to signal the cash dispenser to dispense cash to the customer upon approving the cash advance.

5           The input device may be further configured to provide input signals indicating that a cash advance is desired and indicating an amount for the cash advance. For example, the input device may be a numeric keypad. The input device also may include a card reader configured to provide the electronic processor with an account number associated with the cash advance. Actuation of the input device may  
10 correspond to insertion of a card into the card reader, and the customer identifier may be an account number associated with the card.

          The apparatus may be configured to contact a human operator for assistance when the database of customer information does not contain data about the customer. To this end, the apparatus may include a communications port having a connection,  
15 such as a connection over the public telephone network, to a location at which the operator is located.

          The biometric device may be a camera, such as a digital video camera, configured to obtain an image of the customer's face, and the biometric information may be the image of the customer's face. The camera may be configured to obtain the  
20 image of the customer's face in response to actuation of the input device by the customer. The stored biometric information may include stored images of customers' faces, and comparing the received biometric information to the stored biometric information may include comparing an image of the customer's face from the database of customer information to the image of the customer's face produced by the camera  
25 to confirm the identity of the customer. The apparatus also may include a second camera configured to obtain a second image of the customer's face, and the processor may be configured to compare the first and second images when confirming the

identity of the customer. The apparatus also may include lights positioned to illuminate the customer's face to improve an image obtained by the camera.

5 The customer identifier may be an identification number, and may include multiple symbols. The input device may be configured to produce an input signal corresponding to one symbol in response to each actuation of the input device by the customer.

10 The apparatus may include an output device for providing information to the customer. For example, the input device and the output device may be provided by a touch screen display. The output device may be a speaker, and the apparatus may include a voice synthesizer connected to the speaker and configured to provide spoken information to the customer through the speaker. The input device may be a numeric keypad.

The apparatus may be configured to perform check-cashing transactions. To this end, the apparatus may include a check reader configured to receive and read a  
15 check to be processed. The electronic processor may be configured to perform check-cashing transactions by receiving the input signals from the input device, receiving information about the check to be processed from the check reader, accessing the database of customer information to obtain data about the customer, determining automatically whether to accept or reject the check based on the input signals, the  
20 received information about the check, and the data about the customer, and upon accepting the check, signalling the cash dispenser to dispense cash to the customer.

The apparatus may be configured to determine automatically whether to accept or reject the check by applying a set of business rules. The business rules may be defined generally to permit the processor to accept the check if the customer has  
25 used the apparatus previously to cash a previous check for a similar amount from a payor associated with the check to be processed.

The apparatus also may be configured to accept the check when the database of customer information includes a record for the customer and other criteria

are met. For example, the processor may be configured to accept the check when criteria stored in the record for the customer are met. The processor may be configured to reject the check when a criterion stored in the record for the customer is not met.

5           The storage device also may include a database of payor information, and the processor may be configured to accept the check when the database of customer information includes a record for the customer, criteria stored in the record for the customer are met, the database of payor information includes a record for a payor of the check, and criteria stored in the record for the payor are met. The processor may  
10 be configured to reject the check when a criterion stored in the record for the payor is not met.

A system for providing pinless, automated cash advances may include one or more instances of the apparatus along with a remotely located service center. Each apparatus may include a first communications device connected to the processor, and  
15 the service center may include a second communications device configured to communicate with the first communications device. For example, the second communications device may be configured to communicate with the first communications device using a public telephone network.

The processor may be configured to confirm the identity of the customer  
20 when the database of customer information includes a record for the customer and the received biometric information matches the stored biometric information, and to contact the remotely-located service center for assistance when the database of customer information does not include a record for the customer. The processor also may be configured to contact the remotely-located service center for assistance when  
25 the received biometric information does not match the stored biometric information.

The service center may include a storage device including a central database of customer information, the customer information including stored biometric information, and an electronic processor connected to the second communications

device and the storage device. The processor of the service center may be configured to receive information about a customer from the second communications device, the information including received biometric information for the customer, and to access the central database of customer information to obtain data about the customer  
5 identified by the customer identifier, the data including biometric information stored in the central database for the customer. The processor then may compare the received biometric information to the biometric information stored in the central database for the customer, and control the second communications device to transmit to the first communications device an indication of whether the received biometric information  
10 matches the biometric information stored in the central database for the customer.

The processor of the service center may be configured to contact a human operator at the service center for assistance when the received biometric information does not match the biometric information stored in the central database for the customer. The database of customer information stored on the storage device of the  
15 apparatus may include only a partial subset of the customer information of the central database of customer information.

The service center also may include a display device for use by a human operator. The processor of the service center may be configured to display information about a transaction on the display device when the received biometric  
20 information does not match the biometric information stored in the central database for the customer, to permit the human operator to confirm the customer's identity. For example, the operator may ask the customer to remove a hat or sunglasses and to look directly into the camera. The operator also may verify the customer's identity by referencing a database that includes information about the customer's current and  
25 previous addresses, telephone numbers, and neighbors. Access to a database suitable for this purpose is available, for example, from Integrated Database Software, Inc. of Villa Park, Illinois.

The first communications device may be configured to initiate communications with the second communications device and to reject communications initiated by the second communications device.

5 An apparatus for providing pinless cash advances may be implemented using a retrofit module connected to an automated teller machine having an input device and a cash dispenser. The retrofit module is configured to be connected to the automated teller machine and includes an input/output port configured to receive an input signal from the input device of the automated teller machine. The input signal corresponds to a customer identifier and is generated in response to actuation of the  
10 input device by the customer. The retrofit module also includes a biometric device, a storage device and an electronic processor. The biometric device (e.g., a camera) is configured to receive biometric information about the customer (e.g., an image of the customer's face). The storage device includes a database of customer information, including stored biometric information for the customer. The electronic processor is  
15 connected to the input/output port, the biometric device, and the storage device, and is configured to receive the input signal from the input/output port and the biometric information from the biometric device. The processor then accesses the database of customer information in response to the input signal to obtain data about the customer identified by the customer identifier, including stored biometric information for the  
20 customer. The processor compares the received biometric information to the stored biometric information, and transmits a notification message to the input/output port. The notification message indicates that the customer's identity has been established when the received biometric information matches the stored biometric information.

The systems also may be configured to provide short term loans. When  
25 configured in this manner, a system verifies a customer's identity using the described biometric techniques. After verifying the customer's identity, the system verifies that the customer's checking account is in good standing. If so, the system provides the customer with a form that sets forth the terms of the loan and prompts the customer to

insert a check for the loan amount. After verifying that the check is for the proper amount and has been signed, the system provides the customer with cash in the amount of the loan.

5 The system delays cashing the check for an agreed-upon payment period (e.g., one week). The customer may extend the payment period by making a payment before the period expires. If the customer does not pay off the loan or make a payment before the payment period expires, the system cashes the check. If the customer pays off the loan, the system voids the check and disposes of it. In some implementations, the system may return the voided check to the customer.

10

For a better understanding of the invention and to show how the same may be carried into effect reference is now made by way of example to the accompanying drawings in which:

Figs. 1 and 2 are front and side views of an automated check-cashing unit.

Figs. 3 and 3A are block diagrams of the check-cashing unit of Fig. 1.

15 Figs. 4, 5, 5A and 5B are block diagrams of check-cashing systems using the check-cashing unit of Fig. 1.

Figs. 6A and 6B are flow charts of a procedure implemented by an ATM of the check-cashing unit of Fig. 1.

20 Fig. 7 is a flow chart of a procedure implemented by a processor of the check-cashing unit of Fig. 1.

Figs. 8A and 8B are flow charts of a procedure implemented by a centralized services center of the check-cashing system of Fig. 5.

Fig. 9 is a table of business rules.

25 Fig. 10 is a screen display of the centralized services center of the check-cashing system of Fig. 5.

Figs. 11A-11R are sub-screens of the screen display of Fig. 10.

Figs. 12A and 12B are tables of referrals and actions to be taken by the central services center of the check-cashing system of Fig. 5 in response to the referrals.

5 Figs. 13A-13S are flow charts of procedures implemented by the centralized services center in responding to the referrals of Fig. 12A.

Figs. 14A-14P are flow charts of procedures implemented by the centralized services center in performing the actions of Fig. 12B.

Figs. 15A-15L are data structures employed by the check-cashing system of Fig. 5.

10 Figs. 16A-16F are screen displays of a point-of-sale unit.

Figs. 17-19 are flow charts of procedures implemented in providing ATM transactions.

Fig. 20 is a flow chart of a procedure implemented in providing loan transactions.

15

Pinless credit card advances may be performed in conjunction with a check cashing system such as is described below. The advances also may be performed using a system that performs traditional or cardless ATM transactions, or using a dedicated system.

20

An automated check-cashing unit 100, also referred to as a point-of-sale ("POS") unit, is illustrated in Figs. 1 and 2. The check-cashing unit 100 includes a touch-screen display 105, a numeric keypad 110, and a speaker 115 that permit the unit to communicate with a customer. A telephone handset 120 permits communication between the customer and a remote operator. A pair of digital video  
25 cameras 125 produce images of the customer that are used to verify the customer's identity.



The check-cashing unit 100 also includes a check reader 130 into which the customer's check is inserted for processing. When the unit 100 decides to cash the customer's check, a cash dispenser 135 provides cash to the customer and a printer 140 provides the customer with a receipt. In general, the cash dispenser 135 may include four cash drawers, with the drawers containing, respectively, \$1, \$5, \$20 and \$100 denominations. If desired, the cash dispenser 135 also may include a change dispenser. An optional card reader 145, though not needed for the check-cashing function of the unit 100, permits the unit 100 to provide credit card cash advances and banking functions (e.g., withdrawals from a checking or savings account).

10       The check-cashing unit 100 also includes privacy screens 150 that provide the customer with a degree of privacy while using the checking unit. Lights 155 are positioned so as to illuminate the customer's face in a way that permits the video cameras 125 to produce high quality images.

15       An optional base 160 permits the check-cashing unit 100 to be configured as a stand-alone unit (as shown in Figs. 1 and 2). The base 160 may be removed to configure the check-cashing unit 100 as a counter-top unit (not shown). The check-cashing unit also may be mounted within a wall, configured as a drive-through unit, or configured in other ways.

20       Referring to Fig. 3, the check-cashing unit 100 is controlled by a processor 300. The processor 300 receives input from the customer through the input portion of the touch screen 105 and through the keypad 110. The processor provides information to the customer through the display portion of the touch screen 110. The processor also may use a voice synthesizer 305 to speak to the customer through the speaker 115.

25       A video card 310 permits the processor 300 to receive images from the cameras 125. The processor 300 uses these images to identify the customer. In some instances, the processor may receive information about the customer's identity from the card reader 145.

A deposit processing module 315 connected to the check reader 130 provides the processor with information about the customer's check. Using a database loaded from a storage device 320 into memory 325, the processor verifies the customer's identity and determines whether the processor is authorized to cash the customer's check. If the processor concludes that it is authorized to cash the customer's check, the processor instructs a cash dispensing module 330 to dispense an appropriate amount of cash to the customer through the cash dispenser 135. The processor 300 provides the customer with a receipt through the printer 140. As indicated by the dashed lines in Fig. 3 and illustrated in Fig. 3A, the touch screen 105, the keypad 110, deposit processing module 315, the check reader 130, the cash dispensing module 330, the cash dispenser 135, the printer 140, and the card reader 145 may be implemented using a commercially-available ATM 350, such as the DPATM Model Number 5675 available from the NCR Corporation. The processor 300 may communicate with a processor 355 (Fig. 3A) of the ATM through, for example, an ethernet connection provided by an Ethernet card 360 (Fig. 3A), and may communicate according to the TCP/IP protocol.

When the processor 300 is unable to verify the customer's identity, or is unauthorized to cash the customer's check automatically, the processor may transmit information about the customer and the customer's check to a remotely-located centralized services center ("CSC") through the public telephone network (see Fig. 4). Personnel at the CSC, or a computer at the CSC, then attempt to verify the customer's identity and authorize cashing of the customer's check.

An ISDN card 335 allows communication between the processor 300 and the CSC. The ISDN card 335 also is connected to the handset 120 to permit the customer to speak with personnel at the CSC, if necessary. In some circumstances, the ISDN card 335 may be replaced with a cellular modem or similar device.

As noted above, the optional card reader 145 may be included to permit the unit 100 to provide traditional ATM transactions, such as deposits, withdrawals, and

balance inquiries. In addition, the unit 100 may be configured to provide cardless ATM transactions. When the unit 100 is configured in this way, the unit 100 stores account information for customers. The unit 100 then identifies the customer using biometric information as described above. When necessary, the unit 100 invokes the CSC or personnel at the CSC to confirm the customer's identity. After identifying the customer, the unit 100 contacts a gateway of a service network to determine whether the customer may perform a desired transaction (e.g., to determine whether the customer's account includes sufficient funds). When a unit 100 is used for ATM or credit card transactions, the security/identification aspect of the transaction processing network is isolated from the approval/processing aspect of the network.

As noted, the unit 100 may provide credit card cash advances. When the customer selects a credit card cash advance from an options menu and inserts a credit card into the card reader 145, the unit 100 prompts the customer to enter the amount of the advance and the customer's social security number or other identification number. Optionally, the unit 100 may use the card number as the identification number so that the customer does not need to manually enter an identification number.

If the customer is requesting a cash advance for the first time (i.e., if a record does not exist for the customer and the customer's credit card number), the unit 100 contacts the CSC. An operator at the CSC confirms the customer's identity and verifies that the customer is the person whose name appears on the credit card. While confirming the customer's identity, the operator contacts the verification network for the credit card to obtain an authorization code for the cash advance. If the customer's identity is confirmed and approval for the transaction is obtained, the operator approves the cash advance by notifying the unit 100 to dispense the requested amount of cash.

A record for the customer is created at the CSC and the unit 100. The record may be indexed according to the credit card number, the customer's identification number, or both. The record includes the customer's identification

number, the credit card number, the customer's name, and biometric information in the form of an image of the customer's face. The record also may include information about the credit card account, such as the credit limit.

Depending upon system configuration, the customer may request subsequent  
5 cash advances upon inserting the credit card and entering an identification number, upon inserting the credit card (without entering an identification number), or upon entering an identification number or a credit card number (without actually inserting the credit card). In each case, the unit 100 uses the biometric information stored in the record to confirm the customer's identity and contacts the credit card verification  
10 network for an authorization code. The system also may be configured to require operator intervention for transactions that exceed a threshold amount.

Referring to Fig. 4, a large number of POS units 100 may communicate with a CSC 400 through the public telephone network 405. The POS units 100 automatically cash checks and perform transactions that meet certain criteria, while  
15 deferring to the CSC 400 for authorization to cash checks or perform transactions that do not meet the designated criteria. For security, the POS units 100 initiate all calls to the CSC and do not accept incoming calls. Similarly, the CSC accepts calls only from known POS units 100.

As shown in Fig. 5, a server 500 at the CSC 400 receives and processes  
20 calls from the POS units 100. The server, which generally has more available information than does a particular POS unit 100, may determine that the check should be cashed and may provide an indication to that effect to the calling POS unit 100. When the server 500 is unable to automatically cash a check, and determines that a call needs the attention of CSC personnel, the server identifies an available operator  
25 and directs information about the call through an Ethernet connection 505 to the operator's workstation 510. The operator then decides whether to cash the check and sends an appropriate signal to the calling POS unit 100. The server may direct calls based solely on operator availability, but also may consider other criteria. For

example, the server may direct a call to an operator fluent in a language identified by the customer when accessing the POS unit 100.

As shown in Fig. 5A, in one implementation, hardware of each POS unit 100 is implemented using an NCR 5675 ATM, two digital cameras, an Intel Pentium processor operating at 166 MHz, 32 megabytes of memory, a 2.5 gigabyte hard drive, an Ethernet card providing a coaxial cable connection between the ATM and the processor, an ISDN card, a Matrox video capture card, speakers, a telephone handset, and BRI ISDN telephone service. In the same implementation, hardware of the CSC is implemented using twenty three lines of PRI ISDN telephone service; a Lucent Definity telephone switch; an Ascend router; two fast Ethernet 100BaseT hubs; an IBM 704 PC Server configured as a call handler (2x200 MHz, 256 MB memory, 2.14 GB Hard drive, redundant power supply, fast Ethernet card); an IBM 704 PC Server configured as a file server (4x200 MHz, 256 MB memory, 27.06 GB RAID-1 Disk, 24/48 GB internal tape auto loader, redundant power supply, fast Ethernet card); an IBM Server Rack 24 inch (14" color display, 101 keyboard); a Best uninterruptable power supply ("UPS") 5.3 kVA with the capability to run 5 hours without power for the telephone switch, router, fast Ethernet hubs, server rack, file server, and call handler; and forty workstations. Each workstation may be implemented using an Intel Pentium processor operating at 200 MHz, 32 MB memory, a 2.5 GB hard drive, a 101 Keyboard, a mouse, a fast Ethernet card, a 17" touch screen monitor, a phone handset, and a UPS.

Connectivity in the implementation of Fig. 5A may be provided as shown in Fig. 5B. The ATM is connected to the POS processor through an Ethernet coaxial cable. The POS unit dials into the CSC using a BRI ISDN line. The CSC receives calls on a PRI ISDN going into the Definity switch. The Definity switch connects to the Ascend router using PRI ISDN. The Ascend router connects to the CSC call handler using a fast Ethernet Hub 100BaseT. Finally, the call handler, file server, and workstations are connected by a separate fast Ethernet 100BaseT hub.

Referring to Figs. 6A, 6B, 7, 8A and 8B, when performing check-cashing transactions, the ATM 350, the processor 300, and the CSC 400 operate according to interacting procedures, with the ATM 350 operating according to a procedure 600, the processor 300 operating according to a procedure 700, and the CSC operating  
5 according to a procedure 800. As described below, these procedures may be modified when the system is configured to perform credit card or ATM transactions. Initially, the ATM 350 displays a screen that permits the customer to select an appropriate language (e.g., English or Spanish) and waits for the selection from the customer (step 605). When the customer selects the language (step 610), the ATM 350 prompts the  
10 customer to enter the customer's social security number or other identification number. After the customer enters the social security number (step 615), the ATM 350 prompts the customer for the amount of the check and the customer enters the amount (step 620).

Next, the ATM 350 prompts the customer to endorse the check and to  
15 insert the check into the check reader 130 (step 622), and the customer inserts the check (step 625). The check processing module 315 of the ATM 350 scans the check to produce images of the front and back of the check, validates the MICR ("magnetic ink character recognition") code on the check, and reads designated zones of the check (step 630). If the customer has failed to endorse the check, as indicated by the image  
20 of the back of the check, or has inserted the check incorrectly (step 632), then the ATM returns the check to the customer and prompts the customer to endorse the check (if necessary) and to reinsert the check (step 634). If the check has been endorsed and properly inserted, the ATM 350 then displays an image of the front of the check to the customer (step 635) and validates the contents of the check using optical character  
25 recognition ("OCR") (step 640). Using the recognized amount of the check, the ATM then calculates the difference, if any, between the recognized amount of the check and the amount entered by the customer (step 645).

Next, the ATM 350 sends information to the processor 300 (step 650). The information sent includes the customer's social security number or other identification number, the images of the front and back of the check, MICR information, information as to whether the contents of the check passed the validation step, the check amount  
5 read by OCR, the check amount entered by the customer, and the difference, if any, between the two amounts. The ATM then prompts the customer to remove any hat, sunglasses, or other items that would obscure the customer's face (step 652) and waits for a response from the processor 300. The message may be accompanied by an animated character that removes its hat and sunglasses.

10 Referring to Fig. 7, upon receiving and validating the information from the ATM 350 (step 705), the processor 300 attempts to identify the customer (step 710). To this end, the processor uses identification software that identifies a person based on an image of the person's face. An example of software that is suited for this purpose is the TrueFace CyberWatch software available from Miros, Inc., of 572 Washington  
15 St. #18, Wellesley, MA 02181. This software is described by Miros, Inc., in the Programmer's Manual For TrueFace Version 2, which is incorporated by reference.

The identification software compares an image of the customer produced by a camera 125 with an image stored in conjunction with the customer's identification number in a database stored on the storage device 320. The image is produced when  
20 the customer enters the first digit of the customer's social security number or other identification number to ensure that the customer is looking at the camera. The image from the second camera 125, though not used for comparison with the stored image, is used to verify that the image from the first camera is an image of the customer rather than an image of a picture held in front of the camera. The ATM displays the  
25 "remove hat and sunglasses" message because the presence of a hat or sunglasses can reduce the ability of the identification software to identify the customer. The identification software also may compare the image of the customer's face with a

database of images associated with "bad" customers (i.e., customers who have previously submitted bad checks or who have a record of doing so).

Other types of biometric identification software could be used. For example, the identification software could identify the customer using a fingerprint or  
5 palmprint, DNA analysis, a retinal scan, or an analysis of the customer's voice.

If the identification software approves the customer (i.e., if the customer's image matches the image stored with the customer's identification number) (step 715), the processor determines whether data associated with the customer and the customer's check satisfy a set of business rules stored on the storage device 320 (step 720).

10 The business rules 900 used by the processor in one implementation are illustrated in Fig. 9. These business rules, which are intended to be illustrative only, include a set of criteria 905 and a set of values 910. In general, when checking the business rules, the processor references a payor database and a payee database to obtain information about the customer (the payee) and the customer's employer (the  
15 payor). If the transaction violates any one of the business rules, then the processor 300 is not authorized to automatically cash the customer's check, and must seek authorization from the CSC 400.

If the check satisfies the business rules (step 725), the processor 300 determines the fee to charge the customer and the payback amount (i.e., the amount of  
20 cash that the customer will receive) (step 730). The processor 300 then sends this information to the ATM 350 and waits for a reply (step 732).

Referring to Fig. 6B, upon receiving the fee and payback amount (step 660), since the check has not been rejected (step 665), the ATM 350 displays the fee and payback amount for verification by the customer (step 667). The ATM 350 then  
25 sends a transaction request message to the processor 300 (step 669). Based on the customer's response, the transaction request message indicates to the processor that the transaction should either be continued or cancelled. If the customer has not accepted the transaction (step 671), the ATM 350 returns the customer's check (step 673). The



ATM 350 then ends the transaction (step 675) and waits for another customer (step 605). If the customer has accepted the transaction (step 671), the ATM 350 waits for a transaction reply message from the processor 300.

5 Upon receiving a transaction reply (step 677), the ATM 350 dispenses the appropriate amount of money. The ATM 350 then sends a confirmation to the processor 300 (step 679) and ends the transaction (step 675).

10 If, as discussed below, the processor 300 sends a rejection message in response to the first request (step 665), the ATM 350 displays a rejection message to the customer (step 685), returns the check to the customer (step 690) and ends the transaction as noted above. In some instances, the ATM 350 may retain the rejected check. For example, an operator at the CSC 400 may signal the ATM 350 to retain the rejected check if the operator determines that the check has been stolen.

15 Referring again to Fig. 7, upon receiving a response from the ATM 350 (step 734), the processor 300 sends a reply to the ATM 350 (step 736) and waits for a confirmation. Upon receiving the confirmation (step 738), the processor 300 records the transaction and updates the database located on the storage device 320 (step 740). The processor then waits to receive a new set of data from the ATM (step 705).

20 If the identification software does not approve the customer (i.e., if the customer's image does not match the stored image, or if there is no stored image for the customer's identification number) (step 715), the processor 300 initiates a call to the CSC 400 (step 745) and determines whether data associated with the customer and the customer's check satisfy the business rules (step 747). The processor 300 then gets a bitmap ("BMP") file of the customer's image (step 749) for transmission to the CSC 400. The processor also initiates a call to the CSC (step 750) and gets the BMP file  
25 for the customer (step 749) if the identification software approves the customer (step 715), but the check does not satisfy the business rules (step 725).

After initiating a call, the processor 300 establishes a connection to the CSC 400 using an ISDN line (step 755). The processor uses one channel of the line to

transmit a data packet about the customer and the customer's check to the CSC 400 (step 759). The data packet includes the information sent from the ATM 350 to the processor 300 (i.e., the customer's social security number or other identification number, the images of the front and back of the check, MICR information, information  
5 as to whether the contents of the check passed the validation step, the check amount read by OCR, the check amount entered by the customer, and the difference, if any, between the two amounts), the BMP file including an image of the customer, the results of the identification procedure, and the reason that the transaction is being sent to the CSC.

10           The processor uses the other channel of the line to establish a video conferencing connection between the POS unit 100 and the CSC 400. In one implementation, this connection includes bidirectional audio and unidirectional video, with still images being transferred periodically from the POS unit 100 to the CSC 400. Other implementations may include unidirectional or bidirectional real-time video.

15           Next, the processor 300 waits for a response from the CSC with respect to the current customer (step 760). While waiting for the response, the processor 300 uses any available bandwidth of the connection between the POS unit 100 and the CSC 400 to provide the CSC 400 with information about any transactions that the processor has independently processed (see, e.g., step 738) since the last call from the  
20 processor to the CSC.

Referring to Fig. 8A, the CSC 400 processes each call from a POS unit 100 according to the procedure 800. Upon receiving a call (step 805), the server 500 of the CSC 400 validates a security code associated with the call. Each POS unit 100 is encoded with a unique serial number which that is maintained at the CSC. This  
25 encrypted serial number serves as an authorization key to obtain CSC approvals and is transmitted with every transaction originating from the POS unit 100. At preset intervals, a new serial number is transmitted to the POS unit 100 for further security.

If the security code is invalid, the server 500 notifies the POS 100 and terminates the call.

After validating the security code, the server 500 receives the data packet for the transaction from the POS unit 100 (step 815). The server 500 searches a payor database for the payor of the check (e.g., the customer's employer) (step 820). The  
5 server searches the payor database according to the routing number and the account number printed on the check and provided by the check processing module of the ATM.

If the server 500 finds the payor in the payor database (step 825), the server  
10 500 determines whether the payor has a good payment status (step 827). If the payor does not have a good payment status, the server 500 indicates that the transaction should be rejected (step 829).

If the payor has a good payment status, or if the server does not find the payor in the payor database, the server 500 searches a payee database for the customer  
15 (step 831). The server 500 searches the payee database according to the customer's identification number. If the server 500 finds the customer in the payee database (step 833), the server 500 determines whether the payee has a good status (i.e., whether the customer has a history of depositing good checks) (step 835). If the customer does not have a good payment status, the server 500 indicates that the transaction should be  
20 rejected (step 837).

If the customer has a good status (step 835), and the payor is an established payor with a good status (step 839), the server verifies the transaction against a set of business rules (step 841). The business rules may be identical in content to the business rules 900 used by the processor 300 (see Fig. 9). However, as discussed  
25 below, each business rule includes an identifier, known as "a referral reason", to be displayed to a CSC operator when the rule is violated, and a list of actions that the operator is to take in response to the referral reason. By comparison, the processor

300 of the POS unit can be seen as taking the action of contacting the CSC in response to each referral reason.

5 If the transaction passes the business rules (step 843), the server 500 indicates that the transaction should be accepted (step 845). Thus, the server 500 may automatically accept transactions that the POS unit 100 is unauthorized to accept. For example, if a customer who typically uses a POS unit in a first location switches to a POS unit in a second location, the POS unit in the second location may not have information about the customer in the POS unit's database. For this reason, the POS unit will be unable to identify the customer and, accordingly, will be unauthorized to  
10 cash the customer's check. By contrast, the server 500 will maintain a much larger database with information about customers who use any POS unit. For this reason, the server 500 will be able to identify the customer and authorize the transaction.

If the server 500 is unable to find the customer in the payee database (step 833), is unable to find the payor in the payor database (step 839), or if the transaction  
15 does not satisfy the business rules (step 843), the server sends the transaction to the workstation 510 of the next available operator (step 847) and waits to receive a message from the operator.

Referring to Fig. 8B, upon receiving a call from the call handler (step 849), the operator's workstation 510 provides the operator with the graphical user interface  
20 ("GUI") 1000 illustrated in Fig. 10 (step 850). The GUI 1000 provides the CSC operator with all information from the POS unit that is needed make a decision about the worthiness of the transaction. This information includes information about the payor, information about the payee, including the current and file image of the payee, an image of the check, and an indication as to why the transaction was rejected. In  
25 general, the GUI is a series of tabs with each reason that the transaction was not automatically approved being highlighted. The GUI is in an inactive state until it receives a request from a POS unit for approval. The workstation 510 responds to

actions of the operator by displaying appropriate sub-screens of the GUI. These subscreens are illustrated in Figs. 11A-11R.

Referring again to Fig. 8B, the CSC operator responds to the referrals (step 855) by taking actions (step 860) that may include, among other actions, accepting the transaction, rejecting the transaction, or requesting identification of the user. If the operator accepts the transaction, rejects the transaction, or requests identification of the user, a message is sent to the call handler (step 862).

As noted above, while the CSC operator processes the transaction, the server 500 takes advantage of any available bandwidth of the connection between the POS unit 100 and the CSC 400 to obtain from the processor 300 information about any transactions that the processor has independently processed since the last call from the processor to the CSC (step 865). After retrieving all such data, the server 500 may use any other available bandwidth to update the databases of the POS unit 100.

Referrals that may be provided to the CSC and the actions taken by the operator in response to those referrals are illustrated in Fig. 12A, with the actions that are identified by numbers in Fig. 12A being identified in more detail in Fig. 12B. Flow charts of referral responses are provided in Figs. 13A-13S. Flow charts of actions are provided in Figs. 14A-14P.

Referring again to Fig. 8A, upon receiving a message from the CSC operator (step 870), or after accepting (step 845) or rejecting (step 829 or 837) the transaction, the call handler sends an appropriate message to the POS unit 100 and waits for a response (step 872).

Referring again to Fig. 7, if the message received from the CSC is an identification request (step 767), the POS unit 100 makes a further attempt to identify the customer (step 769) and transmits a resulting BMP file to the CSC 500 (step 771). If the further attempt is unsuccessful, the server 500 may make a further attempt to identify the customer. The server 500 may be able to identify the customer even though the POS unit 100 could not because the server has access to a larger database

than does the POS unit 100. For example, a customer who normally uses a different POS unit may not appear in the payee database of the current POS unit, but would appear in the payee database of the CSC. In this circumstance, the current POS unit would have no image against which to compare the customer's image, while the server  
5 would have such an image. The server 500 then passes the BMP file and the results of the identification to the operator workstation 510 for use by the operator in taking additional actions (step 860 of Fig. 8B).

If the message received from the CSC is not an identification request (step 767), the processor 300 determines whether the transaction has been approved or  
10 rejected (step 773). If the transaction has been rejected, the processor 300 ends the call to the CSC 400 (step 775) and notifies the ATM 350 (step 779).

If the transaction has been approved (step 773), the processor 300 determines the fee to charge the customer and the payback amount (i.e., the amount of cash that the customer will receive) (step 777). The processor 300 then sends this  
15 information to the ATM 350 and waits for a reply (step 779). Because operator intervention was required, this fee may differ from the fee that would have been calculated had the processor automatically approved the transaction.

Upon receiving a transaction verification result from the ATM 350 (step 781), the processor 300 sends a transaction reply message to the ATM 350 (step 783)  
20 and waits for a transaction confirmation message from the ATM. Upon receiving a transaction confirmation message from the ATM, the processor 300 records the transaction and updates the database located on the storage device 320 (step 787). The processor 300 then sends a transaction completed or cancelled message to the CSC 400 (step 789) and ends the call to the CSC 400 (step 791).

25 Referring again to Fig. 8A, upon receiving a reply from the processor 300 (step 874), the server 500 records the transaction and updates the server's databases (step 875).

For tracking purposes, a check record associated with each check being handled by the CSC includes a status code, a check disposition code, and an operator code. A status code of "A" indicates that the check is waiting to be handled by an operator or a supervisor, and a status code of "C" indicates that the check has been  
5 processed by an operator or a supervisor and that the POS unit has performed the appropriate function in response. Check disposition codes of 11, 12, 21, 22, 31, 32, 41 and 42 indicate that the check was accepted ("n1") or rejected ("n2") by the POS unit ("1n"), CSC automatic verification ("2n"), a CSC Operator ("3n") or a CSC  
10 Supervisor ("4n"). The operator code is blank until the active check has been assigned to a specific operator, and thereafter identifies that operator. Other data structures used by the POS unit 100 and the CSC 400 are illustrated in Figs. 15A-15L.

Sample screen displays produced by the ATM 350 of a POS unit 100 are illustrated in Figs. 16A-16F. Arrows between the various screens indicate the sequence and the conditions under which the screens are displayed.

15 The software implemented by the CSC 400 may be described with reference to several different modules. The first module, referred to as the call handler, includes one instance per active call and receives messages from the POS unit. Functions implemented by the call handler include reformatting and/or writing a POS message to the CSC server and identifying the message type of the message. If the message is for  
20 a CSC operator, the call handler instantiates an instant check evaluator that attempts to automatically approve or reject the check associated with the message. If the message is for a CSC supervisor, the call handler places the message into a POS to CSC table. If the message is a photo or check image, and the related check is being handled by an operator or a supervisor (i.e., the check disposition code for the related check is "30"  
25 or "40"), the call handler updates an image display window for the operator or supervisor. The call handler also sends CSC mailbox items that are addressed to the POS unit, and terminates the call when a live call is completed by the CSC operator and all mail for the POS unit is sent.

As noted above, the instant check evaluator attempts to automatically approve or reject a check. The evaluator receives a store number and transaction number from the call handler and evaluates the business rules to determine if the check should be automatically accepted or rejected, and changes the check disposition code to show the results of the evaluation (i.e., "21" indicates automatic approval, "22" indicates automatic rejection, and "30" indicates that operator intervention is required).

An operator transaction manager module routes messages between the other modules. When one or more checks need to be processed by an operator (i.e., there are checks with disposition codes of "30"), and one or more operators are available, the operation transaction manager reads from the oldest check to be processed to the newest check to be processed, and determines for each check whether a qualified operator (e.g., an operator who speaks the appropriate language) is available. If a qualified operator is available, the operation transaction manager places the operator's number into the operator code for the check and passes information about the check to the operator.

A CSC operator module provides information about a check to the operator. The CSC operator module also provides the operator with any other information needed to evaluate the check. Once the operator makes a decision about the check, the CSC operator module changes the disposition code for the check to an appropriate value (i.e., "31" is approved, "32" if rejected, and "40" if referred to a supervisor) and takes an appropriate action.

A CSC supervisor module carries out functions similar to those of the operator transaction manager and the CSC operator module, but does so for the supervisor(s) rather than the operator.

The various software modules communicate with each other with messages passed between and among the modules. The messages may be formatted as: module from, module to, date, time, type, priority, store number, transaction number, and text, where the module from and module to entries may equal: ATM (the automated teller



machine), POS (the point of sale unit), CAM (the camera) and CSC (the central service center), and where "text" is one or more comma delimited fields.

Fig. 17 illustrates a procedure 1700 that may be implemented by an ATM of a POS unit that is configured to provide, in addition to the check-cashing functions  
5 described above, cardless ATM transactions, traditional ATM transactions, and credit card cash advances. Initially, as in the procedure 600, the ATM displays a screen that permits the customer to select an appropriate language (e.g., English or Spanish) and waits for the selection from the customer (step 1705). When the customer selects the language (step 1710), the ATM asks the customer whether a check-cashing transaction,  
10 an ATM transaction, or a credit card cash advance is desired (step 1715). In some implementations, steps 1705-1715 may be circumvented by insertion of a credit card or an ATM card. In these implementations, a record associated with the card indicates the type of card and the desired language. If the customer selects a check-cashing transaction (step 1720), the ATM prompts the customer to enter the customer's social  
15 security number or other identification number and proceeds with check processing as discussed above with reference to Figs. 6A, 6B, 7, 8A and 8B (step 1725).

In another variation, the ATM prompts the customer for an identification number or credit card number instead of asking the customer whether a check-cashing transaction, an ATM transaction, or a cash advance is desired. The processor of the  
20 POS unit then determines whether the customer is a check cashing customer, an ATM customer, or a credit card customer based on information in the customer's record, which is indexed in accordance with the customer's identification number or credit card number. If the record indicates that the customer performs multiple types of transactions, the processor instructs the ATM to ask the customer what type of  
25 transaction is desired.

If the customer selects an ATM transaction or a credit card transaction, the ATM performs an ATM/credit card identification procedure to confirm the customer's identity (step 1730). If the identification is successful (step 1735), the ATM prompts

the customer for instructions as to the ATM or credit card transactions to be performed (step 1740). The ATM then contacts a network provider (step 1745) to determine whether the requested transaction is authorized. For example, the ATM may contact the network provider to determine whether the customer's bank account includes  
5 sufficient funds to cover a withdrawal requested by the customer, or whether the customer has sufficient credit available to permit a cash advance. Finally, the ATM performs any authorized transactions, such as dispensing a withdrawal, accepting a deposit, or providing a cash advance (step 1750).

If the identification is unsuccessful (step 1735), the ATM issues a rejection  
10 message to the customer (step 1755). After processing a check (step 1725), performing authorized credit card or ATM transactions (step 1750), or rejecting an ATM or credit card customer (step 1755), the ATM waits for the next customer to arrive (step 1705).

If, instead of selecting a language (step 1710), the customer inserts an ATM  
15 card in the card reader (step 1760), the ATM prompts the customer to enter a personal identification number (PIN) (step 1765). If the customer enters the correct PIN for the inserted card (step 1770), the ATM prompts the customer for instructions (step 1740) and proceeds as discussed above.

If the customer enters an incorrect PIN for the inserted card (step 1770), the  
20 ATM determines whether the customer has exceeded a permitted number of incorrect entries (step 1775). For example, the system may permit the customer to make three attempts at entering the correct PIN. If the customer has not exceeded the permitted number of entries, the ATM prompts the customer to enter the PIN (step 1765). If the customer has exceeded the permitted number of entries, the ATM issues a rejection  
25 message to the customer (step 1755). The ATM may be configured to either return or keep the customer's card upon issuing a rejection message.

Instead of selecting a language (step 1710) or inserting an ATM card (step 1760), the customer may insert a credit card into the reader (step 1780), where the

card's identity as a credit card may be determined from the card number. When this occurs, the ATM attempts to identify the customer (step 1730) and proceeds as discussed above.

ATM identification (step 1730) is performed according to the procedure  
5 1800 illustrated in Fig. 18. Initially, the ATM prompts the customer to enter the customer's identification number (e.g., account number or social security number) (step 1805). This step may be circumvented when the customer has inserted a credit card or an ATM card by obtaining the credit card or ATM account number directly from the card and using the account number as the customer's identification number.  
10 Next, the ATM sends the identification number to the processor of the POS unit (step 1810). The ATM then prompts the customer to remove any hat, sunglasses, or other items that would obscure the customer's face (step 1815) and waits for a response from the processor.

Upon receiving the identification number from the ATM, the processor  
15 attempts to identify the customer (step 1820). To this end, the processor uses the identification software described above that identifies a person based on an image of the person's face. As noted above, the identification software compares an image of the customer produced by a camera 125 with an image stored in conjunction with the customer's identification number in a database stored on the storage device 320. As  
20 also noted above, other types of biometric identification software could be used. For example, the identification software could identify the customer using a fingerprint or palmprint, DNA analysis, a retinal scan, or an analysis of the customer's voice.

If the identification software approves the customer (i.e., if the customer's image matches the image stored with the customer's identification number) (step  
25 1825), the processor notifies the ATM of this approval and the ATM proceeds to step 1735 of Fig. 17. If the identification software does not approve the customer (i.e., if the customer's image does not match the stored image, or if there is no stored image for the customer's identification number), the processor initiates a call to the CSC

(step 1830). The processor then gets a bitmap ("BMP") file of the customer's image (step 1835) for transmission to the CSC.

After initiating a call, the processor establishes a connection to the CSC using an ISDN line (step 1840). The processor uses one channel of the line to  
5 transmit a data packet about the customer to the CSC (step 1845). The data packet includes the identification number, the BMP file including an image of the customer, and an indication that the transaction is being sent to the CSC based on the results of the identification procedure. The processor uses the other channel of the line to establish a video conferencing connection between the POS unit and the CSC.

10 The processor then waits for a response from the CSC (step 1850). While waiting for the response, the processor uses any available bandwidth of the connection between the POS unit and the CSC to provide the CSC with information about any transactions that the processor has independently processed since the last call from the processor to the CSC.

15 Referring to Fig. 19, the CSC processes the call from the POS unit according to the procedure 1900. Upon receiving a call (step 1905), the server of the CSC validates a security code associated with the call, as described above. After validating the security code, the server receives the data packet for the transaction from the POS unit (step 1910). The server 500 searches the payee database or similar  
20 databases for ATM and credit card transactions according to the customer's identification number (1915). If the server 500 finds the customer (step 1920), the server attempts to identify the customer using the identification software to compare the BMP file sent with the data packet to an image of the customer stored in the database (step 1925).

25 If the identification is successful (step 1930), the server sends the results to the processor at the POS unit (step 1935). If identification is unsuccessful, the server sends an identification request to the processor at the POS unit and waits for a reply (step 1940).

Referring again to Fig. 18, upon receiving a message from the CSC (step 1855), the processor of the POS unit determines whether the message is an identification request (step 1860). If the message is an identification request, the processor makes a further attempt to identify the customer (step 1865). If the attempt is unsuccessful (step 1870), the processor transmits the resulting BMP file to the CSC (step 1875) and waits for a response from the CSC (step 1850).

If the message received from the CSC is not an identification request (step 1860), or if the new identification was successful (step 1870), the processor ends the call (step 1880) and notifies the ATM of the contents of the message. The ATM then proceeds to step 1735 of Fig. 17.

Referring again to Fig. 19, upon receiving a BMP file in response to an identification request, the server at the CSC makes a further attempt to identify the customer (step 1945). The server may be able to identify the customer even though the POS unit could not because the server has access to a larger database than does the POS unit. For example, a customer who normally uses a different POS unit may not appear in the payee database of the current POS unit, but would appear in the payee database of the CSC. In this circumstance, the current POS unit would have no image against which to compare the customer's image, while the server would have such an image. If the identification is successful (step 1950), the server sends the results to the processor at the POS unit (step 1935).

If identification is unsuccessful (step 1950), the server sends the transaction to the workstation of the next available operator (step 1955) and waits to receive a message from the operator. The server also sends the transaction to the workstation when the customer's identification number is not found in the server's payee database (step 1920).

The operator's workstation displays information about the transaction to the operator (step 1960). When the identification is unsuccessful, this information may include the image stored for the customer along with the image generated by the POS

unit. The operator may compare these images and make a determination about whether the customer actually is who the customer purports to be. The workstation also may provide the operator with other information about the customer to permit the operator to query the customer about the customer's identity. When the server has no  
5 record of the customer's identification number, the operator may communicate with the customer to determine whether the customer has entered the correct number. In either case, the operator responds to the displayed information by sending an approval or rejection message to the server (step 1965), or by passing the transaction along to a supervisor as described above. The server then sends the response to the processor at  
10 the POS unit (step 1935).

Other uses to which the system may be put include, but are not limited to: paying bills, extending loans, producing rent-to-own contracts, filing tax returns, or dispensing social security or other government benefits. For payment of bills, a cash  
15 acceptor or a similar device may be incorporated into the POS unit. Similarly, the system could be configured to perform wire transfers or to dispense money orders or telephone cards.

Other embodiments are within the scope of the following claims. For example, in another embodiment, the check processing module may be eliminated from the POS unit to form a checkless POS unit. The checkless POS unit may be  
20 located on the premises of, for example, a large factory or refinery, and may be used to distribute employee pay without requiring the distribution of employee paychecks. For such a use, an employer transfers funds corresponding to the payroll to an account associated with the CSC and notifies system administrators at the CSC of payroll amounts for different employees. The system administrators then enter these payroll  
25 amounts into records for the employees and download the records to appropriate POS units. An employee may use a checkless POS unit located on the employer's premises or any other POS unit to receive pay.

When an employee uses the system to collect pay, the POS unit and, where necessary, the CSC confirm the employee's identity as discussed above. The POS unit then distributes the payroll amount to the employee. In some implementations, the system may be configured to permit the employee to request less than the payroll amount to the employee and to hold the remainder of the payroll amount until a later request is made.

Another embodiment may be configured to provide short term loans. To obtain such a loan, a customer writes a check for the loan amount, which typically is in the form of \$100 increments. The system then provides the customer with cash corresponding to the loan amount less any processing fees. The system delays cashing the check until the loan period expires. The system also permits the customer to extend the loan period by paying an extension fee.

Fig. 20 illustrates a procedure 2000 that may be implemented by an ATM of a POS unit that is configured to provide short term loans along with other functions, such as check cashing, cardless ATM transactions, traditional ATM transactions, and credit card cash advances. For ease of discussion, the procedure 2000 lists only steps associated with providing loans. However, it should be understood that the procedure could be expanded to provide additional transaction types, and that most systems would provide other transactions along with the short term loans.

Initially, as in the procedure 600, the ATM displays a screen that permits the customer to select an appropriate language (e.g., English or Spanish) and waits for the selection from the customer (step 2005). When the customer selects the language (step 2010), the ATM notifies the customer of available transactions (step 2015). In some implementations, steps 2005 and 2010 may be circumvented by insertion of a credit card or an ATM card. In these implementations, a record associated with the card indicates the desired language.

When the customer selects a loan transaction (step 2020), the ATM prompts the customer to enter the customer's social security number or other identification number (step 2025). The ATM then performs an identification procedure to confirm the customer's identity (step 2030). In particular, the system verifies the customer's  
5 identity using the biometric techniques described above.

If the identification is successful (step 2035), the ATM prints out a document setting forth the terms of the loan (step 2040). The document may be generated using a receipt printer, or may be generated using a separate, dedicated printer. The ATM may further instruct the customer that insertion of a signed check  
10 constitutes acceptance of the terms of the loan.

Next, the ATM prompts the customer to insert a signed check for the loan amount (step 2045). Generally, loans are made in increments of \$100. This simplifies the generation of transaction fees and subsequent amount verification. The ATM analyzes the check to ensure that it is signed and to determine the amount of the loan  
15 (step 2050). In some implementations, the ATM may prompt the customer to separately enter the amount of the loan.

If the check is in good order (step 2055), the ATM contacts a banking network (step 2060) to verify that the customer's checking account is in good standing. (The account number for the checking account is obtained from analysis of the check.)  
20 If the checking account is in good standing (step 2065), the ATM dispenses cash to the customer (step 2070). In general, the amount dispensed equals the loan amount less a processing fee.

In general, the system returns to display of the language prompt (step 2005) after dispensing cash (step 2070), determining that the account is not in good standing  
25 (step 2065), or determining that the check is not in good order (step 2055), or after an unsuccessful identification (step 2035). The system may take remedial steps prior to aborting the transaction. For example, the system may contact a central services center



to attempt to confirm the customer's identity after an unsuccessful identification or to explain to the customer how to correct the check.

5 The system holds the check for a period corresponding to the term of the loan (e.g., two weeks) prior to cashing the check. The customer may extend the period by paying additional fees corresponding to an interest rate associated with the loan. If the customer pays off the loan in its entirety, the system returns or destroys the customer's check.

10 Cardless and pinless automated financial transactions, cardless automated payroll distribution, short term loans, and pinless credit card cash advances may be provided by a retrofitted automated teller machine. Traditional automated teller machines include an input device, a card reader, and a cash dispenser. Such a machine may be retrofitted to provide cardless transactions by connecting a retrofit module to the machine. In general, the retrofit module includes an input/output port, a biometric device, a storage device, and an electronic processor. The input/output port is  
15 configured to receive an input signal from the input device of the automated teller machine. The input signal corresponds to a customer identifier and is generated in response to actuation of the input device by the customer or insertion of a credit card or ATM card. The biometric device (e.g., a camera) is configured to receive biometric information about the customer (e.g., an image of the customer's face). The storage  
20 device includes a database of customer information, including stored biometric information for the customer. The electronic processor is connected to the input/output port, the biometric device, and the storage device, and is configured to receive the input signal from the input/output port and the biometric information from the biometric device. The processor then accesses the database of customer information in  
25 response to the input signal to obtain data about the customer identified by the customer identifier, including stored biometric information for the customer. The processor compares the received biometric information to the stored biometric information, and transmits a notification message to the input/output port. The

notification message indicates that the customer's identity has been established when the received biometric information matches the stored biometric information.

5 All of the components of the retrofit module may be positioned in a single housing suitable for mounting on top of the automated teller machine or in a wall above the automated teller machine. Alternatively, the input/output port, storage device and processor may be configured to be positioned within the automated teller machine while the camera or other biometric device is positioned in a convenient location near the automated teller machine. When an automated teller machine includes an internal video camera for surveillance purposes, this camera may be used  
10 to obtain an image of the customer. In this instance, the biometric device of the retrofit module would constitute a connection between the camera and the electronic processor of the module.

The techniques described are not limited to any particular hardware or software configuration; they may find applicability in any computing or processing  
15 environment that may be used for cashing checks or performing similar transactions. The techniques may be implemented in hardware or software, or a combination of the two. Preferably, the techniques are implemented in computer programs executing on programmable computers that each include a processor, a storage medium readable by the processor (including volatile and non-volatile memory and/or storage elements), at  
20 least one input device, and at least one output device. Program code is applied to data entered using the input device to perform the functions described and to generate output information. The output information is applied to one or more output devices.

Each program is preferably implemented in a high level procedural or object oriented programming language to communicate with a computer system.  
25 However, the programs can be implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language.

Each such computer program is preferably stored on a storage medium or device (e.g., CD-ROM, hard disk or magnetic diskette) that is readable by a general or

special purpose programmable computer for configuring and operating the computer when the storage medium or device is read by the computer to perform the procedures described in this document. The system may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the  
5 storage medium so configured causes a computer to operate in a specific and predefined manner.

CLAIMS:

1           1. An apparatus for providing pinless, automated cash advances,  
2 comprising:  
3           an input device, the input device being configured to generate an input  
4 signal corresponding to a customer identifier in response to actuation of the input  
5 device by a customer;  
6           a biometric device configured to receive biometric information about the  
7 customer;  
8           a storage device including a database of customer information, the customer  
9 information including stored biometric information; and  
10          an electronic processor configured to:  
11           receive the input signals from the input device,  
12           receive biometric information from the biometric device,  
13           access the database of customer information to obtain data about the  
14 customer, the data including stored biometric information for the customer,  
15           compare the received biometric information to the stored biometric  
16 information,  
17           contact a verification network to request authorization for a cash  
18 advance, and  
19           when the received biometric information matches the stored  
20 biometric information to a degree sufficient to confirm the customer's identity, and  
21 upon receiving authorization from the verification network, approving the cash  
22 advance.

1           2. The apparatus of claim 1, further comprising a cash dispenser, wherein  
2 the electronic processor is configured to signal the cash dispenser to dispense cash to  
3 the customer upon approving the cash advance.

1           3. The apparatus of claim 1 or 2, wherein the input device is further configured  
2 to provide input signals indicating that a cash advance is desired and indicating an  
3 amount for the cash advance.

1           4. The apparatus of claim 3, wherein the input device comprises a numeric  
2 keypad.

1           5. The apparatus of claim 4, further comprising a card reader, wherein the  
2 card reader is configured to provide the electronic processor with an account number  
3 associated with the cash advance.

1           6. The apparatus of any preceding claim, wherein:  
2           the input device comprises a card reader,  
3           actuation of the input device comprises insertion of a card into the card  
4 reader, and  
5           the customer identifier comprises an account number associated with the  
6 card.

1           7. The apparatus of any preceding claim, wherein the apparatus is configured to contact  
2 a human operator for assistance when the database of customer information does not  
3 contain data about the customer.

1           8. The apparatus of any preceding claim, wherein the biometric device comprises a  
2 camera configured to obtain an image of the customer's face, and the biometric  
3 information comprises the image of the customer's face.

1           9. The apparatus of claim 8, wherein the camera is configured to obtain the  
2 image of the customer's face in response to actuation of the input device by the  
3 customer.

1           10. The apparatus of claim 8 or 9, wherein:  
2 the stored biometric information comprises stored images of customers'  
3 faces, and  
4 comparing the received biometric information to the stored biometric  
5 information comprises comparing an image of the customer's face from the database of  
6 customer information to the image of the customer's face produced by the camera to  
7 confirm the identity of the customer.

1           11. The apparatus of claim 8, 9 or 10, wherein the camera comprises a digital video  
2 camera.

1           12. The apparatus of claim 8, 9, 10 or 11, comprising a second camera  
2 configured to obtain a second image of the customer's face, wherein the processor is  
3 configured to compare the first and second images when confirming the identity of the  
4 customer.

1           13. The apparatus of claim 8, 9, 10, 11 or 12, comprising lights positioned to  
2 illuminate the customer's face to improve an image obtained by the camera.

1           14. The apparatus of any preceding claim, comprising an output device for  
2 providing information to the customer.

1           15. The apparatus of claim 14, wherein the input device and the output  
2 device comprise a touch screen display.

1           16.     The apparatus of claim 14 or 15, wherein the output device comprises a  
2 speaker, the apparatus further comprising a voice synthesizer connected to the speaker  
3 and configured to provide spoken information to the customer through the speaker.

1           17. A system for providing pinless, automated cash advances, the system  
2 including the apparatus of claim 1 and a remotely-located service center, wherein:  
3           the apparatus further comprises a first communications device connected to  
4 the processor, and  
5           the service center comprises a second communications device configured to  
6 communicate with the first communications device.

1           18. The system of claim 17, wherein the second communications device is  
2 configured to communicate with the first communications device using a public  
3 telephone network.

1           19.     The system of claim 17 or 18, wherein the processor is configured to confirm  
2 the identity of the customer when the database of customer information includes a  
3 record for the customer and the received biometric information matches the stored  
4 biometric information, and to contact the remotely-located service center for assistance  
5 when the database of customer information does not include a record for the customer.

1           20. The system of claim 19, wherein the processor is configured to contact  
2 the remotely-located service center for assistance when the received biometric  
3 information does not match the stored biometric information.

1           21.     The system of claim 17, 18, 19 or 20, wherein the service center further comprises:  
2           a storage device including a central database of customer information, the  
3 customer information including stored biometric information; and

4 an electronic processor connected to the second communications device and  
5 the storage device, and configured to:

6 receive information about a customer from the second  
7 communications device, the information including received biometric information for  
8 the customer,

9 access the central database of customer information to obtain data  
10 about the customer identified by the customer identifier, the data including biometric  
11 information stored in the central database for the customer,

12 compare the received biometric information to the biometric  
13 information stored in the central database for the customer, and

14 control the second communications device to transmit to the first  
15 communications device an indication of whether the received biometric information  
16 matches the biometric information stored in the central database for the customer.

1 22. The system of claim 21, wherein the processor of the service center is  
2 configured to contact a human operator at the service center for assistance when the  
3 received biometric information does not match the biometric information stored in the  
4 central database for the customer.

1 23. The system of claim 21 or 22, wherein the database of customer information  
2 stored on the storage device of the apparatus includes only a partial subset of the  
3 customer information of the central database of customer information.

1 24. The system of claim 21, 22 or 23, wherein:  
2 the service center further comprises a display device for use by a human  
3 operator, and  
4 the processor of the service center is configured to:



5 display information about a cash advance on the display device to  
6 permit the human operator to confirm the customer's identity when the received  
7 biometric information does not match the biometric information stored in the central  
8 database for the customer.

1 25. The system of claim 21, 22, 23 or 24, comprising a second instance of the  
2 apparatus of claim 1.

1 26. A retrofit module for configuring an automated teller machine having  
2 an input device and a cash dispenser to provide pinless cash advance transactions, the  
3 retrofit module being configured to be connected to the automated teller machine and  
4 comprising:

5 an input/output port configured to receive an input signal from the input  
6 device of the automated teller machine, the input signal corresponding to a customer  
7 identifier and being generated in response to actuation of the input device by the  
8 customer;

9 a biometric device configured to receive biometric information about the  
10 customer;

11 a storage device including a database of customer information, the customer  
12 information including stored biometric information for the customer; and

13 an electronic processor connected to the input/output port, the biometric  
14 device, and the storage device, the processor being configured to:

15 receive the input signal from the input/output port,

16 receive biometric information from the biometric device,

17 access the database of customer information in response to the input  
18 signal to obtain data about the customer identified by the customer identifier, the data  
19 including stored biometric information for the customer,

20                   compare the received biometric information to the stored biometric  
21 information, and  
22                   transmit a notification message to the input/output port, the  
23 notification message indicating that the customer's identity has been established when  
24 the received biometric information matches the stored biometric information.

1               27. The module of claim 26, wherein the biometric device comprises a  
2 camera configured to obtain an image of the customer's face, and the biometric  
3 information comprises the image of the customer's face.

1               28. An apparatus for providing loans, comprising:  
2               an input device, the input device being configured to generate an input  
3 signal corresponding to a customer identifier in response to actuation of the input  
4 device by a customer;  
5               a biometric device configured to receive biometric information about the  
6 customer;  
7               a storage device including a database of customer information, the customer  
8 information including stored biometric information;  
9               a check reader configured to read a check to determine an amount of the  
10 check and an account number associated with the check; and  
11              an electronic processor configured to:  
12                    receive the input signals from the input device,  
13                    receive biometric information from the biometric device,  
14                    access the database of customer information to obtain data about the  
15 customer, the data including stored biometric information for the customer,  
16                    compare the received biometric information to the stored biometric  
17 information,

18                   contact a network provider to determine whether an account  
19 associated with the account number is in good standing, and  
20                   when the received biometric information matches the stored  
21 biometric information to a degree sufficient to confirm the customer's identity, and  
22 upon determining that the account is in good standing, approving the loan in an  
23 amount less than equal to the amount of the check.

29.    An apparatus for providing automated cash advances substantially as  
hereinbefore described with reference to the accompanying drawings.

30.    A method of providing automated cash advances substantially as hereinbefore  
described with reference to the accompanying drawings.



45.

Application No: GB 9914847.0  
Claims searched: 1-30

Examiner: Michael Logan  
Date of search: 15 October 1999

**Patents Act 1977**  
**Search Report under Section 17**

**Databases searched:**

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK CI (Ed.Q): G4H (HTG); G4V (VAK); G4X (X5)

Int CI (Ed.6): G07C 9/00; G07F 7/10, 19/00

Other: Online: WPI, EPODOC, JAPIO

**Documents considered to be relevant:**

Category	Identity of document and relevant passage	Relevant to claims
X,P	EP 0878780 A2 (NCR) whole document relevant	1-6,8-11
X,P	WO 98/35298 A1 (MR PAYROLL) see especially pages 2-9	1 at least
X	WO 98/15924 A2 (SMART-TOUCH) see especially page 5, lines 3-23	1-5 at least
X	US 5386104 (NCR) whole document relevant	1-5 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.